Data Protection Policy and Procedures

September 2023

CONTENTS

DOCUMENT CONTROL

Who is this policy for?

This policy applies to employees (including consultants, temporary and agency staff), Trustees, Members, Academy Advisory Body (AAB) members, volunteers and anyone acting on behalf of Delta Academies Trust (the "**Trust**").

References to "**you**" and "**your**" in this policy refer to employees of the Trust and references to "**we**", "**us**" or "**our**" refer to the Trust itself.

We process personal data about a range of Data Subjects, such as employees, Trustees, pupils / students, those with parental responsibility for pupils / students and suppliers.

This Policy Statement

The aim of this policy statement is to provide an overview of:

- the Data Protection Legislation,
- our responsibility in respect of data protection practice,
- your rights and obligations
- why privacy is so important.

It applies to all actions we take which involve the processing of and working with personal data. We work hard to ensure that personal data is processed in accordance with Data Protection Legislation and in particular the six principles contained in the UK GDPR together with the associated accountability principle.

This policy statement and the supporting policy have been approved by the Audit and Risk Committee of the Trust's Board of Trustees. Its success depends on the co-operation of our employees and the involvement of all staff to help us to meet its requirements.

This Policy is maintained by the Data Protection Officer, who will ensure that it is accurate and up to date. If you are aware that this policy is incorrect or out of date, please inform the Data Protection Officer immediately. The Data Protection Officer can be contacted via DPO@deltatrust.org.uk.

Protective marking

Not protectively marked.

Review date

This policy will next be reviewed before the end of September 2027, or when there are changes to the legislative requirements.

Revision History

REVISION	DATE	DESCRIPTION	AUTHOR
1	Nov 2018	Policy issued.	Emma Mayor
2	Nov 2019	Revised policy approved by Audit and Risk Committee.	Emma Mayor
3	Mar 2021	Policy revised.	Emma Mayor/Amie Carlyle
4	August/September 2023	Policy revised.	Emma Mayor/Amie Wagstaff

1. SUMMARY

1.1 In order to operate as an organisation, we hold Personal Data about employees, suppliers, pupils, students and their family members, and other individuals. The use of personal data is governed by the UK General Data Protection Regulation, (the "**UK GDPR**") and the Data Protection Act 2018 (the "**Data Protection Legislation**").

1.2 We take data protection very seriously and understand the impact that data breaches and misuse of data may have on data subjects as well as on our activities.

1.3 Compliance with this policy is necessary for us to maintain the confidence and trust of those whose personal data we handle.

1.4 Non-compliance with this policy could, in certain circumstances, constitute a serious disciplinary matter.

1.5 We use a number of terms in this policy such as "**Data**", "**Data Subjects**" and "**Personal Data**". These are defined in **Appendix 1** of this policy.

2. DATA PROTECTION OVERVIEW

2.6 Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure it is done fairly and lawfully and in a way which does not adversely affect an individual.

2.7 Data Protection Legislation regulates the processing of personal data. Personal data is data about a living individual, who can be identified from the data itself, or from the data plus other information which is available to us. Data about businesses or organisations is not covered by Data Protection Legislation but data about individuals such as their Trustees, partners, employees, customers and suppliers is.

2.8 We will process personal data in accordance with Data Protection Legislation and good data protection practice. Processing includes obtaining, recording, holding, reading, using or destroying personal data.

2.9 We process personal data for a number of purposes such as the provision of education, training, welfare, maintenance of accounts and records, employee administration and the management of the business. We also use CCTV to monitor and collect visual images in order to provide a safe and secure environment for students, staff and visitors, as well as to protect academy property. It is important to the Trust that we are able to use personal data in this way.

2.10 We will only process personal data relating to individuals for the purposes it was collected for. We will keep a processing record of all processing of personal data we perform (also known as a ROPA (record of processing activity)). We will make sure our privacy notices are kept up to date and reflect the

processing activities we undertake. Please see the appendices to this policy for the Trust Privacy Notices (also known as Fair Processing Notices).

2.11 We will store personal data in a safe and secure manner and only people who really need to use it as part of their work responsibilities will have access to it.

2.12 We will keep personal data up to date. Where a Data Subject reports an inaccuracy in the personal data we hold, we will correct it (unless we know the information is correct) and will inform any recipients of that personal data of the amendments.

2.13 We will keep personal data only as long as is necessary for the purpose(s) it was collected for. Once personal data is no longer required, we will take reasonable steps to securely destroy or erase it. Please see our Personal Data Retention Policy for further information.

2.14 We will avoid collecting sensitive personal data or criminal conviction or offence data, unless absolutely necessary. If we do collect it, we will take extra measures to ensure it is kept safe and secure.

2.15 The Board of Trustees shall have responsibility for compliance of the organisation with Data Protection Legislation and this Policy. The Board of Trustees acting through its Audit and Risk Committee has appointed Emma Mayor as its Data Protection Officer. The Data Protection Officer shall report to the Audit and Risk Committee on the Trust's compliance with data protection legislation and, in particular, shall provide information in respect of its performance against key performance indicators agreed by the Audit and Risk Committee. On the Board of Trustees, Sean Cavan, Chair of the Audit and Risk Committee has specific responsibility for data protection compliance and will present information provided by the Data Protection Officer and/or the Audit and Risk Committee and will notify the Board of Trustees of any data protection related incidents.

2.16 Each academy has a nominated Data Protection Lead. If you have questions or concerns about the operation or interpretation of this policy, please contact your Academy Data Protection Lead in the first instance.

2.17 Any queries from Data Protection Leads at academies should be referred to the Trust Data Protection Officer, who can be contacted via DPO@deltatrust.org.uk.

2.18 The Data Protection Officer will be the main contact for Data Subjects who have any issue relating to the processing of their personal data or who wish to exercise any of their rights as Data Subjects pursuant to the Data Protection Legislation.

2.19 The Data Protection Officer shall be appointed on the basis of their professional qualities, and in particular their knowledge of Data Protection Legislation and practices and their ability to fulfil at least the following tasks:

- to inform and advise the Trust and any third party processor of the Trust's obligations pursuant to Data Protection Legislation and other relevant and applicable laws; and
- to monitor:
  - compliance with Data Protection Legislation and other relevant and applicable Data Protection Legislation
  - the Trust's policies and those of any third-party processor relating to the processing of personal data, including assigning responsibilities, raising awareness and training employees or being responsible for the training of those involved in processing operations; and
  - related audits.
- where required, to provide advice relating to data protection impact assessments and monitoring performance of those data protection impact assessments;
- to co-operate with the ICO; and
- to act as the contact point for the ICO on issues relating to processing, including any prior consultation and to consult, where appropriate, on any other matter.

2.20 The Data Protection Officer must, in the performance of their tasks, have due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2.21 The Trust must ensure (or any third-party processor must ensure) that the Data Protection Officer is involved, in a proper and timely manner, in all issues relating to the protection of personal data.

2.22 The Trust will (or any third party processor will) support the Data Protection Officer to perform their tasks by providing the necessary resources and allowing them to maintain their expert knowledge relating to data protection matters. This may include appointing additional employees to support and assist the Data Protection Officer or ensuring that the Data Protection Officer can attend all relevant and necessary training (whether internally or externally) as he or she deems appropriate.

2.23 The Trust (or any third party processor) must ensure that the Data Protection Officer does not receive any instructions regarding the exercise of their tasks. He or she shall not be dismissed or penalised in any way by us (or any third party processor) for performing his or her tasks.

2.24 The Data Protection Officer will be bound by an obligation of confidentiality concerning the performance of their tasks.

2.25 The Data Protection Officer may fulfil other tasks and duties, but the Trust (or any third party processor) must ensure that such tasks and duties do not create any conflicts of interest with his/her role as Data Protection Officer.

HOW SHOULD PERSONAL DATA BE USED?

2.26 The UK GDPR (Article 5 (1)) outlines six core principles, which broadly set out the way in which personal data should be used. Personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specific, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- Accurate and, where necessary, kept up to date (accuracy);
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation); and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (integrity and confidentiality).

Article 5 (2) also adds that:

- We must be responsible for, and be able to demonstrate compliance with, the six principles outlined above ('accountability').

2.27 You should be aware that failure to comply with the principles may result in a substantial fine.

2.28 Our compliance with this data protection policy and procedures will ensure compliance with the above principles. We will take care to make sure we process data in accordance with our privacy notices.

2.29 Where we process personal data which is particularly sensitive, such as information about a person's health, religion or sex life or data which is otherwise high risk, such as information relating to someone's identity, including national insurance numbers, passport or driving licence details or bank account details, we will handle the data with particular care.

2.30 When we use personal data, we will ensure that it is used to the least extent possible (i.e. we will not do more with it than necessary). Where we use personal data, we will work to ensure that it is accurate and handled in accordance with the security measures outlined by the Data Protection Legislation.

KEEPING DATA SECURE

2.31 We will process personal data securely by ensuring the confidentiality, integrity and availability of personal data is kept secure. We will ensure the level of security we use is appropriate to the risks arising out of the processing.

2.32 We have put in place a number of policies and procedures, which will keep data secure by providing guidance for our staff and contractors as to how personal data should be stored in order to reduce, as far as reasonably possible, the risks involved in processing personal data.

2.33 We will work together with our IT team to ensure that where Trust employees, students, Members and Trustees (or, if applicable, volunteers) need to take

devices containing personal data out of the secured office environment, the device contains sufficient security features (such as encryption) in order to keep the personal data safe and secure. Please see our Online Safety Policy for further information.

2.34 We have put in place other organisational and physical security measures to protect personal data. Please contact your Academy Data Protection Lead or the Data Protection Officer if you have any queries or suggestions.

2.35 Trust employees, Members, Trustees, AAB members, contractors and/or volunteers must take particular care if they process personal data whilst working from home or away from a Trust site or office.

DATA RETENTION AND DESTRUCTION

2.36 Personal data will be retained by us as long as we need to process it or for as long as the law requires us to keep it. Please see Section 11 for further information on data retention.

2.37 When we no longer need data, we will destroy it in accordance with good data protection practice. Please see the Trust Data Retention Policy for more guidance in this area.

2.38 Where we use third party contractors to destroy data, we will only use contractors who can demonstrate relevant experience and accreditations.

2.39 We shall follow the procedure for destruction set out in Section 14.

STUDENT DATA

2.40 As an Academy Trust, we are not covered by the Educational (Pupil Information) (England) Regulations 2005 in respect of access to a pupil or student's educational record. Therefore, any request for personal data made to us about a pupil/student, including by a person with parental responsibility for a pupil or student, will be subject to the Data Protection Legislation.

STAFF DATA

2.41 In the course of our recruitment and employment of staff, we will collect, retain and process various data about them. This may include special categories of personal data and criminal conviction and offence data about employees. We must provide employees with a fair processing (privacy) notice when processing their personal data. This information will be retained for the duration of their employment by us.

2.42 All employment records, including application forms, interview notes, sickness notes, annual leave records, promotion and appraisal notes, training records, disciplinary and dismissal notes and reports, references (whether confidential or otherwise and whether given or received) and general personnel file notes must be processed in accordance with Data Protection Legislation.

2.43 Personnel records and all written information regarding an employee, including appraisal, career progression and discussions regarding salary should be set out in a manner which contemplates that it may be disclosable as personal data under Data Protection Legislation. All records should therefore be clear and fair and, where opinions are expressed, these should be shown to be such.

2.44 We will retain some information about staff after the end of their employment with us, for residual employment-related matters, such as provision of job references, processing applications for re-employment, matters relating to retirement benefits, for dealing with disputes and litigation and to allow us to fulfil contractual and statutory obligations.

2.45 Where we process special category or criminal conviction and criminal offence data in respect of employees, we will do so in accordance with our Appropriate Policy Document (see **Appendix 12**).

2.46 We may for these purposes need to transfer personal data to professional advisers and other persons to whom we have contracted work for these purposes.

2.47 Our Personal Data Retention Policy sets out the categories of staff data we hold and the relevant retention periods.

REQUESTS FOR DATA

2.48 From time to time, individuals may make a request to us for a copy of all or some of the personal data that we hold about them. This is known as a Subject Access Request.

2.49 Requests can be made in writing or orally and should describe the information sought. A form to help ensure we have the information we need to process a subject access request is included as **Appendix 2** to this policy.

2.50 When we receive requests for data, we are required to answer the request without undue delay and within a calendar month.

2.51 If we are asked to provide a copy of some or all of the personal data (or that of a pupil/student at one of our academies by a person with parental responsibility for that pupil/student), we may ask for more information to help us find the information asked for.

2.52 We may also ask for information to help us check that the person making a subject access request is the Data Subject or that they are a person with parental responsibility for a pupil/student and that they have been properly appointed by the Data Subject to ask for the information.

2.53 We reserve the right to obscure or delete information relating to third parties included within documents or information requested, or any information, which is not the requestor's personal data.

2.54 All Data Subject access requests will be considered properly. If applicants are unhappy with the way we handle requests, they should let us know using the complaint form, a copy of which can be found at **Appendix 5.**

2.55 Occasionally other bodies such as the police, the tax authorities and other enforcement agencies may ask for access to personal data we hold. If Delta employees, Members, Trustees, contractors, AAB members or volunteers receive such a request, it must be promptly referred to the Data Protection Officer. Please see Section 12 for further information on subject access requests.

OTHER RIGHTS

2.56 Data Subjects have a number of rights including:

- a right to erasure,
- a right to data portability,
- a right to object to certain processing,
- a right to restrict processing in certain circumstances and
- a right to prevent automated decision-making.
- In certain circumstances, a right to request that the processing of their personal data be restricted.

2.57 We are committed to ensuring Data Subject rights are upheld and we will work hard to make sure these rights can be exercised.

2.58 If you receive any of these types of requests, please refer them to the Data Protection Officer via DPO@deltatrust.org.uk.

DATA BREACH

2.59 A data breach is a breach of security, which leads to the accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.60 In the event of a data breach, please notify the Data Protection Officer immediately who will deal with the breach and try to resolve any issues arising from the data breach. Please see Section 11 for further information about what to do in the event of a breach.

2.61 A data breach log shall be maintained by the Data Protection officer in accordance with Section 11.13.

SHARING DATA WITH OTHER PEOPLE/ORGANISTIONS

2.62 We will not share personal data with a third party or another organisation, unless the Data Subject has given us their authority to do so, or we are otherwise permitted or required to do so by law.

2.63 We will take care to consider whether the Data Subject has given authority for their data to be passed to another organisation before we transmit the data. Where data is being sent to an organisation for them to process the data either

on their own behalf or for us, we will carry out due diligence on that organisation to make sure they have adequate data protection standards and processes.

2.64 We will carry out due diligence, put in place contracts or data sharing protocols or agreements to govern the use of data by the third party to ensure compliance with all relevant legislation and guidance. We must have a contract in place if we share personal data outside the organisation. Please contact Core Finance before entering into any agreement or raising a Purchase Order with a supplier where you need to share data. We will keep a log of all data sharing arrangements we enter into. Please contact the Data Protection Officer or Chief Finance and Operations Officer if you require more information.

TRANSFERRING DATA OUTSIDE THE UK

2.65 The Data Protection Legislation restricts transfers of personal data outside the UK, unless the rights of the individuals in respect of their personal data have an essentially equivalent level of protection as under the Data Protection Legislation, and there is a lawful basis in the Data Protection Legislation for us to transfer personal data outside the UK. A transfer of personal data outside the protection of the UK is referred to as a 'restricted transfer'.

2.66 Where it is necessary to do so, we will ensure any such 'restricted transfer' is carried out in accordance with the requirements of the Data Protection Legislation, in order to ensure that the level of protection to Data Subjects guaranteed by the Data Protection Legislation is not undermined by any such transfer. Restricted transfers are permitted if the data receiver is located in a country or territory which the UK government has confirmed has "**adequacy**" (meaning that the data protection rules and regulations in that country have been deemed to provide adequate protection). These adequacy decisions are subject to review by the UK government.

2.67 If there are no adequacy decisions in place for the country or territory for the restricted transfer, the transfer may still be made if 'appropriate safeguards', as outlined in the UK GDPR, are in place. These include the use of standard contractual clauses or if one of the 'exceptions' set out in Article 49 of the UK GDPR applies.

2.68 In all cases, please consult the Trust's Data Protection Officer (DPO) prior to transferring any personal data outside the UK.

TRAINING

2.69 We will provide relevant staff and temporary workers (including consultants and/or agency staff) with appropriate training, including refresher training, to make sure that data protection queries are dealt with properly and in accordance with this policy and the law.

2.70 We will make sure staff and temporary workers and workers at our processors have adequate training for their roles.

2.71 We will undertake activities to raise the level of awareness of data protection issues within our organisation.

CHANGES TO THIS POLICY

2.72 We reserve the right to change this policy at any time where it is appropriate for us to do so; we will notify individuals of these changes.

2.73 In changing this policy, we will have regard to legislative change, codes of practice, guidance from or approved by the Information Commissioner's Office ("**ICO**"), good data protection practice and case law.

3. NOTIFICATION AND DOCUMENTATION

3.1 Unless an organisation is exempt, it must notify the ICO if it processes personal data. Our registration number is **Z246644X**. It is the responsibility of the Data Protection Officer to keep the notification up to date. Our registration allows us to:

- provide education, training, welfare and educational support services;
- administer Trust property;
- maintain Trust accounts and records;
- undertake fundraising;
- support and manage Trust employees; and
- use CCTV systems to monitor and collect visual images in order to provide a safe and secure environment for students, staff and visitors, as well as to protect academy property.

3.2 We are obliged to keep the notification up to date at all times. Should any of the details provided as part of the notification change, these must be notified to the ICO.

3.3 Failure to notify the ICO could result in a criminal offence being committed by us or a person who has a duty to notify changes to the ICO.

3.4 If you believe the notification does not reflect current use of personal data or if you want to engage in a novel way of processing data, please refer the matter to the Data Protection Officer via DPO@deltatrust.org.uk who will check the notification and arrange for its amendment if necessary.

DOCUMENTATION

3.5 In order to demonstrate our compliance with the accountability principle under the UK GDPR, we maintain various documentation, including:

- a record of processing activities (ROPA);
- a record of all consents obtained;
- an information risk register (as part of the corporate risk register);
- a data breach log;
- a data protection policy (this document);

- an appropriate policy document for the processing of special category and criminal offence data in certain circumstances;
- a data breach policy;
- Data Subject access request log;
- data sharing log;
- transfer risk assessment where the Trust intends to transfer personal data to a somewhere outside the UK where the country to which the data is being transferred is not considered by the UK government to have adequate safeguards for personal data;
- fair processing (privacy) notices; and
- data protection impact assessments, as necessary, for certain projects.

RECORD OF PROCESSING ACTIVITIES (ROPA)

3.6 We will maintain a written record of our processing activities if we process personal data. The ROPA must contain as a minimum the following information for each processing activity involving personal data:

- the name and contact details of the controller (and, where applicable, the joint controller, the controller's representative and the Data Protection Officer);
- the purposes of the processing;
- a description of the categories of the Data Subjects and the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed (including, where applicable, recipients in third countries or international organisations);
- transfers of personal data overseas to a third party or international organisation (where applicable), including the name of the third country or international organisation and, where applicable, the documentation of suitable safeguards;
- the proposed time limits for erasure of the different categories of personal data, where possible; and
- a general description of the technical and organisational security measures taken to protect the personal data.

3.7 The record of processing activities shall be maintained by the Data Protection Officer who shall ensure that it is accurate and up to date. The record of processing activities is available via the Data Protection Officer. If you are aware that the record of processing activities is incorrect or out of date, please inform the Data Protection Officer immediately.

3.8 The record of processing activities must be available to the ICO, if requested.

A RECORD OF CONSENTS

3.9 UK GDPR requires us to keep a record of all consents that we obtain. The record shall state:

- who consented
- when they consented
- what they were told at the time

- how they consented – we should keep a copy of the relevant document or data capture form. If consent was given online, the record should include the date submitted and link it to the relevant version of the data capture form
- Whether they have withdrawn consent.

3.10 The Data Protection Officer shall be responsible for maintaining the record of consents.

AN INFORMATION RISK REGISTER

3.11 UK GDPR encourages a risk based approach to the processing of personal data requiring us to take account of the likelihood and severity of risks posed by our personal data processing operations.

3.12 As part of maintaining good data protection practice, we will maintain an Information Risk Register as part of the Trust Corporate Risk Register. The Information Risk Register is a risk management tool whereby all information risks are identified together with information about how the risk is managed. The aim is minimise threats and maximise opportunities. Management of risks generally fits into one of the following categories:-

- Tolerate the risk;
- Treat the risk;
- Transfer the risk; or
- Terminate (remove) the risk.

3.13 The information in the Information Risk Register includes:-

- Identification of the risk and rating it [low, medium or high];
- What the likelihood of the risk occurring and what the impact would be;
- Who within the Trust owns the risk; and
- Mitigation/correction measures put in place.

DATA BREACH LOG

3.14 A Data Security Breach Notification form is included in **Appendix 3** to this policy, which can be used to report a data breach in order to ensure all the relevant information is gathered.

3.15 A personal data breach record or log will be maintained by the Data Protection Officer who will ensure that it is accurate and up to date. If you are aware that the data breach log is incorrect or out of date, please inform the Data Protection Officer immediately.

3.16 We will make the data breach log available to the ICO or relevant supervisory authority if requested.

AN APPOPRIATE POLICY DOCUMENT

3.17 We will establish and maintain an appropriate policy document in relation to our processing of special category and criminal offence and conviction data

in the circumstances set out in the appropriate policy document (see **Appendix 12**). This document:

- explains the procedures for complying with the data protection principles set out in Article 5 in relation to the relevant special category data;
- explains our policies regarding the retention and erasure of the relevant special category/criminal offence and conviction data processed including providing an indication of the time period which those personal data shall be retained by us.

3.18 A template appropriate policy document is set out in **Appendix 12** to this Policy and a completed copy is maintained by the Data Protection Officer. We shall:

- review and update the document where appropriate; and
- make it available to the ICO on request.

A DATA BREACH POLICY

3.19 This policy will be maintained by the Data Protection Officer who will ensure it is accurate and up to date. If you are aware that this Policy is incorrect or out of date, please inform the Data Protection Officer.

DATA SUBJECT REQUEST LOG

3.20 A log of all Data Subject access requests received, the Subject Access Request (SAR) log, will be maintained by the Data Protection Officer who shall ensure it is up to date.

A DATA SHARING LOG

3.21 A log of all data sharing arrangements which we enter into, the data sharing log, will be maintained by the Data Protection Officer who shall ensure it is up to date. The data sharing log shall contain the information set out in Sections 5.39 - 5.46. Please see Sections 5.33 - 5.41for further information on our data sharing obligations.

TRANSFER RISK ASSESSMENT

3.22 Where we intend to transfer personal data outside the UK, we have to consider the country to which the personal data is being transferred. We can transfer personal data to countries covered by a UK government adequacy decision, to organisations within the USA that are certified under the US-UK Data Bridge or where the transfer is covered by one of the exemptions/derogations (see the section on international transfers starting at Section 5.48).

3.23 We can also transfer personal data to a country where we use appropriate safeguards such as the International Data Transfer Agreement, the UK Addendum or Binding Corporate Rules. However, where we do this, we must complete a Transfer Risk Assessment ("**TRA**") (see **the ICO's TRA tool** **ICO Website: TRA tool**). The role of the TRA is to make an assessment of whether the transfer

increases the risk to people's data privacy and human rights compared to the risk if the information stays within the UK.

FAIR PROCESSING (PRIVACY) NOTICES

3.24 Please see Section 9 below for further information on the contents of the fair processing notice and how the information within it should be made available to Data Subjects.

A DATA PROTECTION IMPACT ASSESSMENT

3.25 Please see Sections 5.16 - 5.24 below for further information on when data protection impact assessments must be carried out and what they must contain.

4. DATA PROTECTION BEST PRACTICE

4.1 We must process personal data in accordance with the Data Protection Legislation. We are responsible for:

- explaining to all relevant staff the importance of data protection;
- providing staff (including temporary staff) with adequate training (where necessary), information, instruction and supervision to ensure personal data is processed in accordance with the Data Protection Legislation;
- assuming overall responsibility for compliance with the Data Protection Legislation;
- selecting someone to be responsible for ensuring compliance with the Data Protection Legislation and making this person known to staff. This person is the Data Protection Officer;
- making sure that when personal data is transferred outside the UK that it is done so in accordance with the requirements of Data Protection Legislation;
- maintaining a record of processing activities (ROPA) which records how personal data is kept and processed (see Section 3.6); and
- maintaining other documentation including a data breach log (please see Sections 3.14 - 3.16).

4.2 You should:

- be aware of the issues regarding data protection and contact the Data Protection Officer if you have any queries in relation to this policy;
- consider the rights of Data Subjects who may be affected by your data processing actions;
- always process personal data in accordance with this policy;
- report any Data Subject access requests, applications in respect of other Data Subject rights or other questions regarding data protection to the Data Protection Officer;
- report any actual or suspected breach of this policy to the Data Protection Officer immediately; and
- report any Personal Data Breach to the Data Protection Officer immediately when you become aware of it.

5. PROCESSING PERSONAL DATA

5.1 All personal data should be processed in accordance with the Data Protection Legislation and this policy.

5.2 Personal data is data relating to an individual. It includes employee data, supplier data, pupil / student data and data relating to people with parental responsibility for pupils / students. It will not include data relating to a company or organisation, although any data relating to individuals within companies or organisations will be covered.

5.3 Examples of personal data are employee details including employment records, any third-party data, for example information relating to an employee of a supplier or any information gathered about a pupil / student or a person with parental responsibility for that pupil / student. Recorded telephone conversations, notes or opinions relating to an individual or the suitability of a particular individual for a task, as well as photographs taken of staff, students and others or CCTV images are all personal data.

5.4 You will process personal data when you obtain, record or hold the information or data or carry out any operation with the personal data. The following arrangements could involve data processing (this is a non-exhaustive list):

- provision of payroll services;
- database management;
- use of your own mobile phone or social media messaging account to discuss work issues;
- use of your own tablet, laptop, smart phone, mobile phone or digital camera to carry out work;
- taking and storing photographs of job applicants, employees, students or their parents/guardians, including taking photographs of you or your colleagues in the office;
- the disposal of old computer equipment containing personal data;
- the disposal of old office equipment such as filing cabinets which contain paper records detailing personal data;
- scanning of personnel, pension or educational records;
- the taking of video surveillance images including through CCTV and ANPR;
- office relocation activities involving the movement of personal data records; and
- disposal of confidential waste containing personal data.

5.5 You should assume that whatever you do with personal data will be considered to involve processing it and must be carried out in accordance with the requirements of the Data Protection Legislation.

5.6 Records and all written information regarding pupils and students should be set out in a manner which contemplates that it may be disclosable as personal data under the Data Protection Legislation. All records should be clear and should represent a fair and accurate record of what has happened.

5.7 Records and all written information regarding an employee, including appraisal, career progression and discussions regarding salary should be set out in a manner which contemplates that it may be disclosable as personal data under the Data Protection Legislation. All disciplinary actions, commentary, reports and any reports relating to a dismissal of an individual should be written in a manner which is fair and accurate.

5.8 You should only process data if one of the processing conditions set out in the UK GDPR applies. The conditions most likely to apply to processing activities are:

- it is necessary to fulfil a **contractual obligation** or as part of the employer/employee relationship (for example, processing the payroll); or
- to fulfil a **public interest task** (i.e. to educate children);
- you have **consent** to do so. If you are relying on consent to process the personal data you must make sure that the specific consent given covers you for the precise reason you want to process the personal data. Any consent relied on must be clear, specific as to the use intended and unambiguous (see Section 5.51); or
- there is another **legitimate reason** to process the personal data. If you rely on this condition for processing personal data, we will need to consider what that legitimate interest is, record it in the processing record and notify a Data Subject of the legitimate interests if we receive a Data Subject access request in respect of the personal data. When we rely on the legitimate interests condition, we must carry out a three stage test called a Legitimate Interest Assessment ("**LIA**") in the form set out in **Appendix 13**. First, the processing must be necessary, second, we must identify the legitimate reason for processing (this can be the controller's or a third party's). Finally, we must carry out a balancing test between the legitimate rights of the controller or relevant third party and the interests and fundamental rights and freedoms of the Data Subject. Only if the individual's interests and rights and freedoms are overridden by ours (or relevant third party's) legitimate interests can we rely on this basis for processing the personal data. We will keep a record of all LIAs we perform. We cannot rely on legitimate interests as a processing condition where we are carrying out processing activities to fulfil our public interest task.

5.9 If one of the conditions above is not satisfied, you should contact the Data Protection Officer, before processing the personal data, to ensure that the Trust can legally carry out the proposed activity.

5.10 If the personal data to be processed includes special category personal data, for example if it relates to an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, you must:

- take particular care of special categories of personal data;
- unless data is being processed in accordance with an employment contract, for medical purposes or in relation to a criminal investigation, you should make sure you obtain the explicit consent of an individual before processing special category data relating to them;

- If explicit consent has not or cannot be obtained (for example, you cannot normally use consent as a reason to process employee data – see Section 5.58), you must ensure that before any special categories of personal data are processed, one of the processing conditions for special categories of personal data set out in the UK GDPR apply. If you are unsure, please contact the Data Protection Officer;
- store all special categories of personal data with appropriate security measures to prevent unauthorised disclosure. Such measures will include lockable cabinets and password protection of automated data, pseudonymisation and encryption of such data; and
- ensure that our processes, procedures, systems, policies for processing special categories of personal data are regularly tested to ensure they are resilient, compliant with and appropriate for the Data Protection Legislation. This will include ensuring that adequate disaster recovery plans are in place at all times and that our systems are regularly tested, assessed and evaluated for their effectiveness in keeping special categories of personal data secure.

5.11 We must only process personal data relating to criminal convictions and offences when that processing is carried out under the control of official authority or is authorised by law.

5.12 Where appropriate, processing of special category data and criminal conviction and offence data must be recorded in the Appropriate Policy Document (see Sections 3.17 - 3.18).

DATA MINIMISATION

5.13 Data minimisation is a key feature of the requirement under UK GDPR to have a data protection by design and default approach to processing personal data. We understand that if we keep more data than we need, that we risk breaching data protection legislation and increase the chances of a personal data breach occurring. If we fail to keep data to a minimum, we also increase the risk of any personal data breach having a significant impact on Data Subjects and our organisation.

5.14 We will regularly review files and the data we process to make sure we keep the data we process to a minimum to fulfil the purpose we are processing those data for. We will ensure that all personal data are regularly reviewed to ensure they are not excessive for the purpose they are being kept for. This requires us to understand what we hold data for. In respect of special category and criminal conviction and offence data, it is particularly important that we review personal data held to ensure it is kept to a minimum.

5.15 We must not collect personal data on the off-chance it may be useful at a future date. The Data Protection Officer will regularly review all forms we have to gather personal data to ensure they gather the minimum required. Where new forms are created which gather personal data, they must be approved by the Data Protection Officer prior to use to ensure they only gather the personal data we need.

DATA PROTECTION IMPACT ASSESSMENTS

5.16 If we consider that a particular type of processing is likely to result in a high risk to the personal data of Data Subjects, we must carry out an assessment on the impact that the proposed processing will have on the protection of personal data. It is the role of the Data Protection Officer to provide advice to the Trust on data protection impact assessments including whether or not to carry out a data protection impact assessment on a particular processing activity and the methodology to be used. Please contact the DPO at DPO@deltatrust.org.uk for more information.

5.17 Examples of where we would be required to conduct an impact assessment include:

- if we process, on a large scale, special categories of personal data,
- transferring personal data overseas outside the UK, for example where personal data is held in software hosted abroad;
- personal data, which if disclosed could lead to fraud or identity theft (such as basic account details, passport, national insurance or driving licence data);
- innovative use or application of technological or organisational solutions;
- datasets that have been matched or combined;
- where we process special category or criminal offence or conviction data; or
- if we systematically monitor a publicly accessible area on a large scale (this may be the case, for example, if we have many CCTV cameras which monitor public areas near our premises).

5.18 We may conduct a single assessment on a number of different processing operations that each present similar high risks.

5.19 As a minimum, a data protection impact assessment must contain:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest(s) we are pursuing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purpose. In other words, do we need to process data in this particular way, and can it be done in a less intrusive, or more restricted manner?;
- an assessment of the risks to the rights and freedoms of Data Subjects;
- the measures envisaged to address such risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Legislation, taking into account the rights and legitimate interests of Data Subjects and other persons concerned; and
- sign off by the Data Protection Officer of the risks and a report of the risks to the Information Governance Steering Group.

5.20 We will conduct impact assessments on the processing operations as required by Data Protection Legislation.

5.21 We may, when conducting an impact assessment, seek the views of Data Subjects on the intended processing operation.

5.22 If there is a change of the risk presented by a particular processing operation, we will carry out a further review to assess whether the processing is being performed in accordance with the impact assessment.

5.23 If a processor is involved in the processing activity we should ask for their assistance in completing the data protection impact assessment. They are under a legal obligation to help us in this regard.

5.24 There is a Trust data protection impact assessment triage and template available to ensure all areas are covered when carrying out a data protection impact assessment. Please contact the DPO via DPO@deltatrust.org.uk for further information on DPIAs.

5.25 If an impact assessment indicates that any processing operation would, in the absence of measures taken by us to mitigate the risk, result in a high risk to the rights and freedoms of Data Subjects, then we must consult with the ICO.

5.26 If the ICO deems that the proposed processing would infringe Data Protection Legislation, for example if we have insufficiently identified or mitigated the risks, the ICO will provide us with written advice. This should be provided within eight (8) weeks of the ICO receiving our request for consultation, but the ICO may extend this period by six (6) weeks, taking into account the complexity of the proposed processing.

5.27 If we consult the ICO in relation to any proposed processing, we must provide it with:

- (where applicable) the respective responsibilities of the controller, joint controllers (if any), and the processors involved in the processing;
- the purposes and means of the intended processing;
- the measures and safeguards provided to protect the rights and freedoms of Data Subjects pursuant to Data Protection Legislation;
- the contact details of the Data Protection Officer;
- a copy of the data protection impact assessment; and
- any other information that the ICO may require.

5.28 We may be required by law to consult with, and obtain prior authorisation from, the ICO in relation to processing for tasks carried out in the public interest, including in relation to social protection and public health.

5.29 The Data Protection Officer shall be responsible for determining whether any consultation with the ICO is required and shall be responsible for liaising with the ICO in respect of any such consultation.

USING DATA PROCESSORS

5.30 Where we use a third party to process any personal data on our behalf (for example, if we use a contractor to destroy confidential information which contains personal data or if we outsource some administration tasks), we must

ensure that the third party does so in accordance with Data Protection Legislation. In particular, before we enter a contract with a processor, we need to ensure that they provide sufficient guarantees regarding their compliance with Data Protection Legislation. We also need to ensure that they do, and will continue to, implement appropriate technical and organisational measures to ensure compliance with the Data Protection Legislation and protect the personal data of Data Subjects. The requirement for us to obtain sufficient guarantees includes:

- ensuring the processor complies with industry standards;
- ensuring the processor has appropriate technical skills to perform its contractual obligations. For example, we must check references and any claimed exemptions;
- checking the processor's UK GDPR documentation, which may include, data protection impact assessments, privacy policies, the information security policy etc. This demonstrates that the processor has an understanding of its obligations under Data Protection Legislation;
- check whether the processor has been the subject of any enforcement action; and
- check adherence to any approved code of conduct or certification scheme.

5.31 We **should not** engage any third party to undertake any processing on our behalf unless we have a formal contract in place. This must include specific information as to their approach to data processing and their measures to ensure the security of processing.

5.32 Under the Trust scheme of delegation, all contracts of this nature must be signed by the Chief Finance and Operating Officer following the completion of due diligence checks.

5.33 We shall undertake periodic audits of processors after the processing arrangement commences (and such other reviews as may be reasonable depending on any change in circumstance), to review data protection practices in order to monitor the continued compliance of the processor with Data Protection Legislation.

5.34 We shall keep copies of due diligence carried out and any ongoing audits and shall report any adverse findings to the Information Governance Steering Group.

5.35 We must not engage any third party to undertake any processing on our behalf unless and until we have entered into a valid, binding written contract with that third party. Any such contract must include, as a minimum:

- the subject matter and duration of the processing that the third party will undertake;
- the nature and purpose of the processing;
- the type of personal data and categories of Data Subjects;
- our rights and obligations under the contract;
- that the processor will only process personal data on our written instructions;

- that persons authorised to process the personal data on behalf of the third party are subject to an appropriate obligation of confidentiality;
- that the processor will take all measures required by Data Protection Legislation relating to the security of processing;
- that the processor will only engage another processor in certain circumstances (see Section 5.36);
- that the processor will assist us (so far as it is possible) in responding to a request made by a Data Subject in exercising any of its rights under Data Protection Legislation (see Section 2.57);
- that the processor will assist us in complying with certain of our obligations set out in the Data Protection Legislation, including:
    - that the processor will, at our discretion, delete or return all of the personal data to us when it ceases to process personal data on our behalf;
    - that the processor will delete any existing copies of the personal data when it ceases to process personal data on our behalf (unless it is required by law to retain a copy); and
    - that the processor will make all information available to us which is necessary to demonstrate its compliance with its contractual obligations, and that it will allow for and contribute to audits and inspections conducted by us or on our behalf.

5.36 A third party processing personal data on our behalf must not use another data processor without first obtaining our prior written authorisation. The Data Protection Officer must provide any such authorisation.

5.37 If a third party is authorised by us to use another processor to carry out specific processing activities on our behalf, that additional processor must be subject to the same data protection obligations as the third party is subject to with us. We should ask the third party to provide a copy of the contract it proposes to enter into with the additional processor before we provide any authorisation.

5.38 We will maintain a written record when we contract a third party to process personal data on our behalf. The third party data processor record is maintained by the Data Protection Officer. The third party data processor record must contain as a minimum the following information**:**

- the name of the processor;
- the processor's address, the name and contact details of the representative of the processor and the contact details of the data protection officer (where applicable);
- a description of the categories of processing;
- whether data is being transferred outside the UK and if so, the country to which it is being transferred and any safeguards that are in place;
- the details of the activity that the processor is performing with the data;
- the details of any contract in place, including the start and end date;
- whether the contract contains a data protection clause; and
- a general description of the technical and organisational security measures in place by the processor.

DATA SHARING

5.39 Data sharing is the term used for the sharing of personal data between different controllers. In common with general practice, the term is not generally used in this policy to cover the processing of data by an employee or third-party processor acting on our behalf.

5.40 Data sharing can take place in a routine or one-off circumstance. When considering any project, we must consider if it will involve data sharing. Where this is the case, we should consider whether we need to conduct a data protection impact assessment.

5.41 Data sharing must always be lawful, fair and transparent. We must make sure that any personal data we share is reasonable and proportionate to the benefit we, or the Data Subjects, receive. Any decision to share personal data should be made by the Data Protection Officer. Prior to any decision to share personal data, we need to review the proposed data sharing exercise and confirm that we have a lawful basis for sharing the personal data. Where special category or criminal offence or conviction data is involved, we need to make sure we have either an Article 9 processing condition or we are otherwise permitted by law. Prior to any data sharing exercise, we must ensure that individuals know what we are using their data for, unless an exemption applies to this right. We should also consider the following questions:-

- What is the data sharing exercise meant to achieve?;
- What information do we need to share and could the aim be achieved without sharing personal data?;
- What risks does the data sharing pose to individuals? Are there any specific risks we should consider such as the sharing involving high risk data or involving exports of personal data outside the UK?;
- Is it right to share personal data in this way?;
- What would happen if we did not share the data?;
- Are we allowed to share the data?;
- Is it ethical to share the data?
- Who needs access to the shared data and do we ensure such access is controlled?;
- When should we share the data?;
- How do we share the data?;
- How can we ensure that the data sharing activity achieves our objectives?; and
- Do we need to undertake a data protection impact assessment for this data sharing activity or review any pre-existing data protection impact assessment to take account of the sharing activity?

5.42 Where we propose to share personal data once a proposed data sharing partner is known, we need to conduct due diligence on that data sharing partner. This should include undertaking the measures referred to in Section 5.30. After the data sharing arrangements commences, we shall undertake reviews of data protection practices (and such other reviews as may be reasonable depending on any change in circumstance) with the data sharing partner to monitor the continued compliance of the data sharing partner with Data Protection Legislation.

5.43 We must enter into a contract or data sharing protocol to govern the principles of the data sharing relationship. Unlike data sharing arrangements with processors, there are no specific provisions within data protection legislation regarding the terms that need to be inserted into data sharing arrangements. However, all data sharing arrangements we enter should include the following:

- A description of the personal data being shared
- Data security provisions both in respect of the transfer of the data and its ongoing use;
- A commitment to comply with Data Protection Legislation;
- A warranty to only use the data for the purpose for which it was shared;
- A commitment to allow individuals to exercise their rights under data protection legislation; and
- A duty on each of the parties to inform each other in the event of a data breach affecting the shared data.

5.44 We should consider including the following into the data sharing agreement.

- Detailed advice on the specific data to be shared so that none is shared accidentally:
- Include provisions that the parties warrant that the personal data being shared is accurate;
- Classification of personal data being shared so that appropriate security can be applied;
- A procedure to ensure appropriate access rights are applied;
- Making sure databases are compatible and additional information is recorded in similar ways;
- Common rules for retention and deletion of personal data, security arrangements dealing with Data Subject access requests and requests to exercise other rights and dealing with questions and complaints;
- Include review dates and review processes to ensure the data sharing arrangements remain effective; and
- Make sure there are provisions dealing with the termination of the data sharing arrangement and the destruction or return of personal data after the termination date.

5.45 Where such provisions are not included within a data sharing agreement. The Data Protection Officer should be notified and make a decision as to whether or not to continue with the data sharing exercise.

5.46 We shall keep a log of all data sharing arrangements we enter into, as a minimum, the following data:

- The data sharing partner;
- The commencement date and end date, if known, of the data sharing arrangement;
- The volume, type and nature of the data being shared;
- The authorising person at our organisation and any key contact points;
- Any retention or deletion dates; and
- The review date for the arrangement and information about any previous reviews.

INTERNATIONAL DATA TRANSFERS

5.47 The transfer of personal data outside the UK increases the risks involved in processing such personal data. When we transfer personal data outside the UK we need to make sure we comply with the requirements for international data transfers set out in Data Protection Legislation. This applies to all personal data transfers including those to our processors and to other controllers.

5.48 We can only transfer personal data outside the UK where:

- We transfer it to a country in respect of which the UK government has made an adequacy ruling. These are the countries within the EEA, Andorra, Argentina, Canada (commercial organisations only), Guernsey, Isle of Man, Israel, Japan (private-sector organisations only), Jersey, New Zealand, South Korea, Switzerland and Uruguay together with EU and EEA institutions, bodies, offices and agencies.
- We transfer the personal data under an exemption (see Section 5.50 below);
- We transfer the personal data using appropriate safeguards. This means that we transfer the personal data either:
  - using an International Data Transfer Agreement (IDTA);
  - using the UK Addendum; or
  - using contractual clauses authorised by the ICO.

5.49 Where we use appropriate safeguards as our basis for transfer we must also complete a Transfer Risk Assessment to ensure that the transfer of the personal data outside the UK does not increase the risk to people's privacy and human rights compared to if the personal data stays within the UK. We will use the ICO Transfer Risk Assessment to inform our review of a proposed international data transfer: TRA tool

5.50 The exemptions/derogations are:

- explicit consent;
- you have a contract with the individual whose data you are transferring and the processing is necessary in order for you to fulfil your obligations under that contract or the transfer is necessary for you to enter a contract or carry out your obligations under the contract and the contract benefits the person whose data is being transferred in circumstances where they are not a party to the contract;
- important reasons of public interest;
- necessary for a legal claim or defence;
- to protect someone's vital interests (these are generally life and death situations);
- public register transfers; and
- one-off transfers which are necessary to meet compelling legitimate interests.

CONSENT

5.51 If processing is based on a Data Subject's consent, we must be able to demonstrate that the Data Subject has given their specific consent to the

particular processing operation. We will therefore keep a record of all consents obtained. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of a Data Subject's agreement to the processing of their personal data.

5.52 For consent to be informed, a Data Subject should be aware of our identity as controller; and the purpose(s) of the processing for which the personal data are intended. When the processing has multiple purposes, consent must be given for all of those purposes.

5.53 If processing is based on a Data Subject's consent, we must keep a record of the consent wording used for each individual. A template consent form is attached as **Appendix 4** to this policy.

5.54 Any consent forms used must be:

- in an intelligible and easily accessible form;
- in clear and plain language;
- without any unfair terms; and
- clearly distinguishable from other matters.

5.55 Silence, pre-ticked boxes or inactivity by a Data Subject must not be construed as a Data Subject providing their consent to the processing of their personal data.

5.56 Prior to giving consent, a Data Subject must be informed that they have the right to withdraw their consent at any time. It must be as easy for a Data Subject to withdraw their consent as it is to give their consent.

5.57 Consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on consent, despite such consent not being necessary for the performance of the contract or service.

5.58 If there is a clear or significant imbalance between the Data Subject and us as controller, consent may not provide a valid legal ground for the processing of that Data Subject's personal data. This means we cannot rely on consent to process employee personal data in relation to the core features of their employment with the Trust.

5.59 If you have any doubts as to whether a Data Subject has validly consented to the processing of their personal data, please contact the Data Protection Officer immediately. You must not process a Data Subject's personal data until we are satisfied that consent has been validly obtained.

CHILDREN'S CONSENT TO USE OF THEIR PERSONAL DATA

5.60 There may be circumstances in which you wish to process a child's personal data using consent as your lawful basis for processing. This may be appropriate if you are able to give children (or their parents) informed choice and control over how you use their personal data.

5.61 Children are individuals, and age ranges are not a perfect guide to the interests, needs and evolving capacity of an individual child.

5.62 You will need to consider the competence of the child (whether they have the capacity to understand the implications of the collection and processing of their personal data). If they do have this capacity then they are considered competent to give their own consent to the processing, unless it is evident that they are acting against their own best interests.

5.63 For children with additional needs, you should also consider the advice of your SENDCO.

5.64 You should also take into account any imbalance of power in your relationship with the child, to ensure that, if you accept their consent, it is freely given.

5.65 Where the child is not competent then, in data protection terms, their consent is not 'informed' and it therefore is not valid. If you wish to rely upon consent in this situation, you need the consent of a person with parental responsibility authority over that child, unless it is evident that it would be against the best interests of the child to seek such parental consent.

5.66 In England, Wales and Northern Ireland there is no set age at which a child is generally considered to be competent to provide their own consent to processing.

5.67 Each pupil / student and the level of their understanding must be judged on a case-by-case basis, but if a pupil / student is aged 13 or over, then we will generally assume that they have the competence to understand and provide consent to the use of their personal data, subject to completion of the competency assessment outlined above.

5.68 The consent of the holder of parental responsibility for a child should not be necessary in the context of preventive or counselling services offered directly to a child.

5.69 If you have any concerns or queries regarding the consent of a child relating to the processing of their personal data, you must contact the Data Protection Officer immediately.

6. INFORMATION, INSTRUCTION AND SUPERVISION

6.1 A copy of this policy will be kept on the Trust SharePoint.

6.2 Data protection advice is available from the Data Protection Officer who will arrange for advice from external advisers if necessary.

6.3 We will ensure that all new staff, particularly those with access to personal data, are advised at the content of this policy as part of their induction arrangements.

6.4 Temporary staff, work placement students and new staff will receive data protection training where they will have access to personal data before they

are allowed to process personal data. Temporary, work placement students and new staff must not be allowed to carry out activities involving the processing of personal data until such training has been undertaken.

6.5 If you consider that any task or work you have been asked to undertake involves the processing of personal data and you are unsure whether or not the task or work would be in breach of Data Protection Legislation or other laws, you should check this with the Data Protection Officer.

6.6 We will work to raise awareness of data protection issues across the organisation. We will regularly run awareness raising activities using a variety of methods including emails, team briefings, posters, handouts and messages on our SharePoint.

6.7 We will ensure that awareness raising messaging is easily accessible and relevant to our staff and our business activities. Awareness campaigns will focus on positive messages on what staff can do to help rather than just dealing with the consequences of getting things wrong.

7. COMPETENCY FOR TASKS AND TRAINING

7.1 We recognise that our employees are a key factor in supporting our effective and efficient operation and helping us to comply with Data Protection Legislation and good practice. We are committed to ensuring employees receive training and development to help fulfil our legal and good practice obligations regarding the processing of personal data. It is the responsibility of the Data Protection Officer to monitor training undertaken and to ensure that such training is in compliance with the organisation's obligations under Data Protection Legislation. The Data Protection Officer shall provide information on training undertaken and proposed to the Information Governance Steering Group together with any agreed KPIs relating to training.

7.2 In the first instance, employees will receive an appropriate "on the job" induction into the organisation. The induction will cover data protection. The level of training will be dependent on your position. Such induction training shall take place within the first week of the commencement of the individual's employment or in any event, prior to the individual processing personal data in the course of their employment. Please see the Trust Induction Policy for further information.

7.3 The training provided will ensure employees as a minimum:

- understand the importance of protecting personal data;
- are familiar with how to keep data secure;
- understand the criminal offences that employees can commit by wrongful processing of personal data;
- are familiar with how to spot and prevent access to personal data by unauthorised persons through, blagging or phishing; and
- are informed of any restrictions placed on employees in respect of their processing of personal data.

7.4 All new employees will be supervised by an experienced employee until they achieve the appropriate standards and efficiency required for our employees. Additional training on data protection issues may be provided as appropriate.

7.5 We shall undertake a training needs analysis (TNA) for each employee in respect of their requirements for data protection training. The TNA shall identify specific data protection training needs to enable employees to perform their roles properly, including any specialist training.

7.6 You should only process personal data where you have received adequate induction/training to do so. This applies equally to full time, part time and temporary employees and work placement students. If you consider you need further or refresher data protection training to carry out a task allocated to you please notify the Data Protection Officer.

7.7 Annual refresher training will be provided.

7.8 It is important we keep a record of your completion of data protection training, including refresher training. This record is kept by the Academy /Human Resources for Core Team. You must notify us of any data protection training you complete so that we can keep your record up to date. If an employee has received data protection training before they join the organisation, it is useful for us to know this, as it is important for us to understand the skill sets of our employees.

8. MONITORING THE USE OF PERSONAL DATA

8.1 We are committed to ensuring this policy is put into practice and that appropriate working practices are being followed. To this end, the following steps will be taken:

- all employees who deal with personal data will be made aware of data protection issues and encouraged to work towards continuous improvement in the way we process personal data;
- spot checks may be carried out to ensure compliance with data protection laws and this Policy; and
- the Data Protection Officer shall submit to the Audit and Risk Committee a report on, amongst other things, the level of compliance with or variance from good data protection practices.
- the Audit and Risk Committee will consider what steps, if any, are necessary in order to improve data protection performance.

8.2 Complaints on our data protection practices may be received from:

- employees;
- suppliers;
- our pupils / students or their family members, carers or guardians; or
- others whose personal data we handle.

8.3 Complainants should be encouraged to complete our Data Protection Complaint Form. Please see the appendices to this policy. However, complaints should be dealt with, even if no complaint form is completed.

8.4 The Data Protection Officer will be responsible for investigating any complaints about our data protection practices in order to deal with any data protection breaches and to see what improvements can be made to prevent recurrences of such breaches. The results of such investigations will be reported to ELT, who will be responsible for ensuring any recommendations are implemented.

9. PROVISION OF FAIR PROCESSING NOTICES

9.1 We must provide fair processing information to Data Subjects relating to the processing of their personal data. The information we are required to provide depends upon whether a Data Subject's information is collected from the Data Subject directly or if the information has been obtained from a source other than the Data Subject.

If we have obtained the personal data from the Data Subject

9.2 We must provide the Data Subject with the following information, to ensure fair and transparent processing:

- who we are and our contact details;
- the contact details of our Data Protection Officer;
- the purposes of the processing and the legal basis for the processing;
- if the processing is necessary for our (or a third party's) legitimate interests, what those legitimate interests are;
- the recipients, or categories of recipients, of the personal data (if any);
- whether we intend to transfer personal data outside the UK, and what safeguards are in place;
- the period that the personal data will be stored, or, if we cannot specify such a timeframe, the criteria we will use for determining such a period;
- the Data Subject's right to:
  - access their personal data;
  - request the rectification or erasure of their personal data;
  - request that the processing of their personal data be restricted; and
  - their right to data portability;
- that if the processing is based on their consent, that they have the right to withdraw their consent to the processing at any time;
- that they have the right to lodge a complaint with the ICO;
- whether there will be any automated decision-making (including profiling) and the logic involved, as well as the significance and envisaged consequences of such processing for a Data Subject and
- whether the provision of their personal data is a statutory or contractual requirement, or it is required to enter into a contract, as well as whether a Data Subject is obliged to provide their personal data and the possible consequences if they fail to provide such personal data.

9.3 Standard privacy notices have been prepared and are included in the Appendices to this document and on individual Academy websites. The Data Protection Officer shall be responsible for ensuring privacy policies are up to

date and made available so the information is provided to a Data Subject. If we intend to further process a Data Subject's personal data for a purpose which is different to that which the personal data was originally collected for, we must update the privacy policy in order to provide the Data Subject with information on this new purpose and with any other relevant information in Section 9.2 that may have changed.

If we have obtained a Data Subject's personal data from a source other than the Data Subject

9.4 We must provide the Data Subject with the same information as set out in Section 9.2 other than the final bullet point, however, we must also inform Data Subjects of:

- the categories of personal data concerned; and
- the source from which their personal data originated, and, if applicable, whether it came from publicly accessible sources.

9.5 We must provide the information set out in Section 9.4 to a Data Subject within a reasonable period of obtaining the personal data, and in any event within one month. We can do this by providing them with the privacy notice in that timescale.

9.6 If we are using the personal data for communicating with a Data Subject, then we must provide the information set out in Section 9.4 no later than the first communication with the Data Subject. This information can be provided in a number of ways including in a statement in our email footer, in an email with the Data Subject (if we are communicating with the Data Subject via email).

9.7 If we envisage disclosing personal data to another recipient, we must provide the information set out in Section 9.4 to the Data Subject no later than when the personal data is first disclosed.

9.8 If we intend to further process a Data Subject's personal data for a purpose which is different to that which the personal data was originally collected for, we must update the privacy policy to provide the Data Subject with information on this new purpose and with any other relevant information in Section 9.4 that may have changed.

9.9 There are certain circumstances when we may not be required to provide the information in Section 9.4 to a Data Subject, including where the Data Subject already has the information. If you are uncertain as to whether or not the information should be provided to a Data Subject, or when it should be provided to a Data Subject, you should contact the Data Protection Officer.

10. HANDLING AND STORING PERSONAL DATA AND DATA SECURITY

10.1 We shall take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data. The UK GDPR requires procedures and technologies to be implemented to maintain the security of all personal data from the point of collection to the point of

destruction. The measures taken should be appropriate for the harm which may be caused by any such accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data. Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- "**Confidentiality**" means that only people who are authorised to use the data can access it;
- "I**ntegrity**" means that personal data should be accurate and suitable for the purpose for which it is processed; and
- "**Availability**" means that authorised users should be able to access the data if they need it for authorised purposes.

DATA SECURITY

10.2 When processing personal data, we must ensure that we implement appropriate technical and organisational measures to ensure a level of security that is appropriate to the risks involved in processing such data.

10.3 This may include, for example, pseudonymising certain personal data (i.e. taking identifying fields in a database and replacing them with artificial identifiers), so that the data is anonymous to the people who receive and hold it, or encrypting certain personal data.

10.4 Implementing appropriate technical and organisational measures also means that we must:

- be able to restore the availability and access to personal data in a timely manner, in the event that there is a physical or technical incident involving any personal data (disaster recovery);
- have a process in place for regularly testing, assessing and evaluating the effectiveness of these measures to ensure the security of our data processing; and
- ensure that, by default, only the personal data which is necessary for each specific purpose of processing is in fact processed.

10.5 We are always looking for ways to improve the security of our processing operations.

10.6 If an employee has any concerns or suggestions in relation to the security of our processing operations, or the technical and organisational measures adopted they should contact the DPO@deltatrust.org.uk.

PAPER RECORDS

10.7 Manual data refers to paper and other non-digital personal data, records (such as copies of photographs or plans).

10.8 Manual records containing personal data must be regularly reviewed in order to ensure that the data contained within them is accurate, not excessive, up to date and adequate for their purpose. All files shall be reviewed on a regular basis for this purpose (at least annually) and a record should be kept of all such reviews.

10.9 Any documents containing personal data or special categories of personal data should not be left on a desk on view when the desk is unattended. For example, do not leave HR records, CVs, pupil/student records, parent/guardian data on desks when you leave your desk, even if it is just for a short time.

10.10 You should not remove paper documents containing personal data from the office. If you need to work away from the office, you must either use your work laptop or use your own device provided you do so as set out in the Trust Online Safety Policy.

TECHNICAL SECURITY MEASURES

10.11 The technology and cyber landscape is constantly evolving. We will ensure that we design, maintain and configure our systems to ensure good cyber security is an integral part of our systems. Our systems will be maintained and updated to deal and adapt to emerging threats and risks.

10.12 We will ensure that we manage our IT assets. We will ensure we know what data and systems we manage and what business needs they support. We understand that without careful planning and diligence, over time systems can grow and it can sometimes be hard to maintain an understanding of all the IT assets within our IT environment. We therefore aim to understand fully all of our assets so we can understand and address the resulting risks. We will undertake regular audits and systems monitoring to ensure we manage our systems and are able to identify and assess any vulnerabilities that may present risks to us. This includes:

- The creation of an asset inventory;
- Ensuring we understand who is responsible for each IT asset;
- Understanding what data is stored and processed and where this happens. Personal data should always be stored electronically on our central systems, or on encrypted corporate devices. Staff must not store personal data on their own electronic devices or at home;
- Understanding the architecture of our systems;
- Maintain a list of suppliers and the assets they manage.

10.13 We will ensure we keep our systems and assets protected throughout their lifecycle. We will establish a vulnerability management process to understand the vulnerabilities we face and to understand which are the most serious in order to prioritise those vulnerabilities. To do this we will:

- Keep our systems updated including through having a software update strategy to ensure we patch and update software and systems in an appropriate and timely manner;
- Develop and maintain a vulnerability management process that ensures we have an up to date understanding of vulnerabilities within our estate. This will include the use of vulnerability scanning systems to help identify and assess vulnerabilities including malware and viruses. We will triage and fix vulnerabilities we identify and will ensure that we prioritise them based on the risks they present;

- Identify and manage legacy equipment and systems where it is not possible to upgrade them.

10.14 We shall control who and what can access our systems and data. We will use appropriate methods to establish and prove the identity of users. We will adopt an appropriate password policy. We will ensure that access rights are minimised and we will use the concept of "least privilege". We will review user accounts regularly for unnecessary privileges and ensure privileged access rights are revoked promptly where they are no longer required. We will monitor accounts to detect potential malicious behaviour.

10.15 We will ensure that we protect personal data where it is vulnerable. We need to protect personal data while it is at rest, in transit and at end of life. This will help us ensure that data is appropriately protected wherever it is, in accordance with the risks it faces. We will make sure we can restore important data from back-ups where access is disrupted for any reason. We will test such back-ups regularly to ensure we know how to restore data from such back-ups. We will securely sanitise old IT equipment and storage media when they are no longer needed for their designated purposes to ensure their disposal does not lead to unauthorised access to personal data;

10.16 We will design our systems so we can detect and investigate incidents. We will maintain appropriate logs so they are available when needed, so we can understand the impact of incidents. This will help us understand what monitoring activities we need to undertake on our systems, networks and services. We will develop and test our incident response plans to ensure that we can respond appropriately where security incidents occur. We will incorporate lessons from incidents and test incidents into organisational improvements.

10.17 If you use a phone or other mobile device which allows access to your work email account, you must ensure it is protected by a passcode which should be kept secure at all times. The passcode should not be easy to guess or use common combinations. If you are concerned that someone may know your passcode, you must change it immediately.

10.18 Where documents containing personal data are held off the network, these must be password protected and must be deleted as soon as operationally possible.

10.19 Where there is a requirement to take a device containing personal data out of the work place, you should store it carefully. Laptops, tablets, smart phones and other mobile devices should be stored securely and not left unattended in cars, trains, in public places or on top of desks or table tops at home left unattended overnight. Should one of these devices be compromised for any reason i.e. theft, you should report this to the Police (where applicable), to Core ICT and the DPO.

10.20 You should ensure that individual monitors are positioned so they do not show confidential information to passers-by or people sitting in adjacent seats in public places. This is particularly important if your PC displays employee, pupil / student data or sensitive data. Where this is not possible, alternative solutions

may be available, such as screens to obscure glass panels in doors or screen shields. PCs must be locked or logged off when left unattended. Note that Trust devices are set to lock automatically after a period of not being used.

10.21 Please see the Trust Online Safety Policy for more details.

ORGANISATIONAL SECURITY MEASURES

GOVERNANCE

10.22 We will put in place management structures to ensure the appropriate processing of personal data. Governance measures include ensuring that at all times a person on the Board of Trustees has responsibility for data protection issues and ensuring they are regularly reported to the Audit and Risk Committee. The appointment of our Data Protection Officer demonstrates our commitment to good governance procedure. We have put in place an inter-departmental information governance group to ensure we review data protection matters on a business-wide basis. This is the Information Governance Steering Group.

MANUAL RECORDS

10.23 You should keep manual (non-digital) records secure by the use of locked cabinets. Access to such records should be restricted to those employees whose job requires access. Where a manual record is in constant use you should take appropriate security measures. These could include securing such records during lunch breaks and outside office hours and positioning desks and screens to prevent inadvertent disclosure.

TELEPHONE ENQUIRIES

10.24 If you deal with telephone enquiries you should be careful about disclosing any personal data held by us. In particular, you should:

- check the caller's identity to make sure that information is only given to a person who is entitled to it;
- suggest that the caller puts their request in writing if you are not sure about the caller's identity or where their identity cannot be checked; and
- refer to the Data Protection Officer for assistance in difficult situations.

10.25 Particular care needs to be taken when speaking to people with parental responsibility about pupils / students, as they may have no legal right of access to the information. If you need advice with regards to information requests and parental responsibility, please contact the DPO.

BUILDING ACCESS

10.26 Building access codes, if applicable, should be kept secret and you should ensure that when you enter the code, it cannot be seen by any third party. Where security passes are in place, all staff must wear their security passes at all times in a prominent, visible position. Do not hold the entry door open for

individuals you do not know or who are not displaying a valid security pass. Any stranger seen in entry-controlled areas should be reported immediately to the Principal/Head of Academy/Site Manager.

STORAGE

10.27 You must store personal data in a manner which enables it to be processed in accordance with the Data Protection Legislation. Files should indicate what information they contain and should be readily accessible (provided appropriate security measures are taken) to enable Data Subject access requests to be handled in accordance with this policy.

DELETION OR DESTRUCTION OF DATA

10.28 Where personal data needs to be deleted or destroyed, adequate measures should be taken to ensure that such data is properly and securely disposed of. This will include the destruction of files and back up files and the physical destruction of manual files.

10.29 The sale or destruction of all IT equipment including PCs, laptops, smart phones and other mobile devices together with storage media should be treated as a data processing activity. This will include even where a device or PC, laptop or device is found to be corrupted. Measures should be taken including the use of specialist contractors who have relevant accreditations to ensure data on IT equipment is forensically wiped.

10.30 Particular care should be taken with the destruction of manual sensitive data (written records) and this may include shredding or giving it to specialist contractors.

10.31 Where data is to be destroyed using third party contractors, due diligence should be undertaken in respect of such contractors, including checking relevant accreditations to ensure that they cover the relevant activities and the checking of references. The destruction of data and equipment containing data is a data processing activity and we must ensure that a contract is in place, which complies with our legal requirements in this regard. The Trust has entered into a central contract for the destruction of confidential paper documents, which applies to all academies and Head Office.

10.32 All equipment or information destroyed shall be recorded using certificates of destruction which record the nature of the data, the reason for destruction, the date and method of destruction and the responsible contractor (if any) which shall be kept by the responsible person. Prior to destruction/deletion, the responsible person must satisfy himself/herself that the data is no longer required, that no work is outstanding on or using the data and that no litigation or internal or external investigation is pending where such data would be required as evidence.

PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

10.33 The UK GDPR requires us to take into account the principles of privacy by design and privacy by default when we process personal data.

10.34 Privacy by Design means that we are required to build privacy into the design, operation and management of any system, hardware, software, business practice, protocol or operation that processes personal data. We should minimise the use of personal data where we can, anonymise or pseudonymise where possible, and as soon as possible.

10.35 The principle of Privacy by Design requires that our default position is to apply the strictest privacy settings to any new product or service that we are proposing to use which processes personal data automatically. Privacy settings should always be set to the most private setting possible. Any requirements to deviate from the most private settings must be submitted for approval to the Trust Information Governance Steering Group (IGSG).

10.36 Privacy assurance, Privacy by Design and Privacy by Default must be embedded into our day-to-day operations. It forms a fundamental element of our organisation's risk structure.

10.37 By ensuring that privacy is at the forefront of our thoughts and is embedded throughout the entire organisation, we will not only reduce the risk of a Personal Data Breach, but we will reduce the time, effort and cost spent dealing with privacy concerns that arise.

SECURITY POLICY UPDATES

10.38 We shall ensure all security policies and procedures are regularly monitored and reviewed to ensure that personal data is being kept securely. Policies and procedures shall be reviewed against good data protection practice including ICO and other regulatory guidance and case law. Where policies and procedures are found to be inadequate, prompt and appropriate action shall be taken in order to rectify such inadequacies. This shall include a review of the security sections and the consideration and implementation of replacement provisions to rectify such inadequacies. We shall notify users of any changes in the Policy.

11. PERSONAL DATA BREACH, NOTIFICATION AND REPORTING

INTRODUCTION

11.1 We will ensure that personal data is stored and used in accordance with this policy and the law. However, breaches may occur despite our best efforts. We are under a statutory obligation to report Personal Data Breaches, which create a risk to Data Subject rights and freedoms to the ICO. It is therefore essential that on discovering a breach has occurred, the breach is reported in accordance with this policy to ensure that the impact of the breach on Data Subjects is minimised and our liability for the breach can be limited as much as possible.

11.2 Reporting and thorough investigation of incidents also helps to ensure that potential risks and problems are identified early and appropriate changes are

made to minimise the possibility of future Personal Data Breaches occurring (including through the sharing of lessons learnt).

WHAT IS A PERSONAL DATA BREACH?

11.3 Data Protection Laws require us to ensure that appropriate technical or organisational measures are used to ensure the security of personal data, including against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

11.4 A Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored or otherwise processed.

11.5 A key feature of a Personal Data Breach is the release (no matter how caused) of personal data to a third party who is not authorised to access, view, hold or otherwise process the information. Examples of Personal Data Breaches would be:

- an employee leaving a piece of personal data about another employee (such as their address, date of birth etc.) on an unattended desk so that other employees who do not have permission to view the information can see it;
- the sending of an e-mail containing personal data (for example a database) to a third party who is not entitled to see it, for example, by entering the wrong email address (this risk can often be mitigated through password protection);
- the loss of a folder of papers or an electronic device;
- the theft of a laptop, tablet, smart phone, mobile or digital device (such as a camera) containing personal data, such as a database or e-mails.

WHO CAN REPORT PERSONAL DATA BREACHES?

11.6 Personal Data Breaches can be reported by:

- the Trust;
- an employee;
- pupils / students, and people with parental responsibility for them;
- anyone whose personal details we hold; and
- a member of the public.

WHAT SHOULD I DO IF I THINK A PERSONAL DATA BREACH HAS OCCURRED?

11.7 If you know, or suspect, that a Personal Data Breach may have occurred, regardless of who is at fault, this must be reported to your Academy Data Protection Lead or to the Trust's Data Protection Officer immediately via DPO@deltatrust.org.uk. In the Data Protection Officer's absence, the Personal Data Breach should be reported to the ELT Education Lead (for an Academy), the Director of ICT or the CEO.

11.8 If there is a Personal Data breach, which creates a risk to Data Subject rights and freedoms, we must notify the ICO, without undue delay and where feasible, no later than 72 hours after having become aware of it.

11.9 We will be aware the breach has happened when we have a reasonable degree of certainty that a security incident has occurred that has led to personal data being disclosed or compromised. We are entitled to a short period of investigation after we hear about the alleged breach to work out if a breach has occurred. This short period should last no longer than 24 hours.

11.10 We are required to notify the ICO, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons (e.g. the disclosure only of personal data to the wrong person but who is nevertheless a trusted person (such as another teacher at the school or at another of the Trust's schools) who subsequently confirms they have deleted the information). The Data Protection Officer shall be responsible for determining whether the Personal Data Breach is likely to result in a risk to the rights and freedoms of natural persons.

11.11 You should also notify the Data Protection Officer if there is a 'near-miss'. Reporting of near misses can help prevent actual incidents of injury, loss or damage occurring. A near miss would occur when, for example, a memory stick is lost which contains personal data but is known to be encrypted.

11.12 The Data Protection Officer shall ensure that all Personal Data Breaches are promptly and adequately investigated, notified to the ICO as soon as possible (where appropriate), resolved and documented.

11.13 The Data Protection Officer will maintain a record of all Personal Data Breaches. This record will contain at least the following information:

- the facts relating to each Personal Data Breach including the nature of the breach, e.g. paper record lost away from the office, the numbers affected and the types of data affected such as email addresses or customer account details including bank account numbers;
- the name and contact details of our Data Protection Officer);
- the effects of the Personal Data Breach (including on the affected Data Subjects) e.g. loss of special category or high-risk information including bank account or medical information; and
- the remedial action taken e.g. advising Data Subjects to reset passwords.

11.14 The surrounding circumstances as to how the breach occurred may be very important. You should consider the following and be ready to provide this information to the Data Protection Officer when reporting the breach:

- when the Personal Data Breach occurred (this will be particularly relevant if the Personal Data Breach involves illegal activity);
- how the data was stored including any relevant security measures relating to the method of storage (for example, paper records in a file or electronic records on a laptop);

- who was responsible for the data at the time of the Personal Data Breach;
- whether a third party processor was involved; and
- how the Personal Data Breach occurred (for example, was the data misplaced or stolen, was it accessed by someone who shouldn't have had access to it or was there some other sort of breach).

11.15 If a third party processor is involved in processing any personal data which forms part of the Personal Data Breach, that processor should be asked to provide all reasonable assistance and cooperation in dealing with and remedying any Personal Data Breach. Under Data Protection Legislation they have a legal obligation to assist.

11.16 The ICO is entitled to request a copy of our data breach log to verify our compliance with the Data Protection Legislation. It is therefore vital that you provide as much information as possible, as quickly as possible, about a Personal Data Breach that you become aware of to the Data Protection Officer and that we keep the data breach log up to date.

NOTIFYING OTHERS

11.17 Under Data Protection Legislation there is a statutory obligation on us to notify affected individuals where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of those individuals. We will notify individuals whose data is involved in the Personal Data Breach in order to allow them to take any necessary steps to mitigate their losses. The Data Protection Officer shall decide whether any individuals should be notified of the Personal Data Breach. However, please be aware that the ICO can require us to notify individuals if we have failed to do so, but it believes the Personal Data Breach creates a high risk even if this was not our assessment of the risks created by the breach.

11.18 In addition to notifying individuals, we will consider notifying the following parties of the Personal Data Breach:

- outside media;
- the police If the Personal Data Breach has arisen as a result of illegal behaviour such as theft, hacking or a denial of service attack; and
- other affected parties including our regulator, stakeholders and our insurers.

11.19 Any decision to notify affected individuals will be based on the requirements of Data Protection Legislation, ICO guidance, whether the Personal Data Breach is likely to result in a high risk to that individual and whether or not notification will assist the individual to mitigate his/her loss arising out of the incident. If an individual is notified of a Personal Data Breach, we must notify them without undue delay. We must also notify the Personal Data Breach to an individual if required to do so by the ICO.

ASSESSING THE RISK

11.20 Once notified of a potential Personal Data Breach, the Data Protection Officer will appoint a team of individuals to investigate the incident. The team is responsible for assessing the risk level of the Personal Data Breach incident and assessing the adverse consequences of the Personal Data Breach to the individuals involved.

11.21 Determining whether or not the breach is a risk requires consideration of the likelihood and severity of the risk caused by the data security breach to individuals. When you consider the risk you should take into account:

- the type of breach;
- the nature, sensitivity and volume of personal data;
- ease of identification of individuals;
- the severity of consequences for individuals;
- special characteristics of the Data Subject; and
- the number of affected individuals.

11.22 The information in Section 11.21 should be used to classify whether a breach is high risk or not. It is more likely a breach will be considered to be high risk where it may lead to physical, material or non-material damage. This would include discrimination, identity theft or fraud, financial loss and damage to reputation. Where the breach involves special category data, criminal offence or conviction data or related security measures, it is much more likely to be regarded as high risk.

CONTAINMENT OF BREACH AND RECOVERY

11.23 Consideration should be given as to whether there is anything that can be done to mitigate the loss (for example, whether any of the data can be recovered).

11.24 We will appoint a multi-disciplinary incident response team to work on containing the Personal Data Breach, if applicable. The team should be given clear instructions as to what their tasks are (for example, they may be instructed to close a weakness in the IT system through which personal data has been released).

11.25 Consideration should be given as to whether there is anything we can do to limit the damage (for example, utilising back up records to restore the data that is the subject of the Personal Data Breach or promptly notifying individuals affected so they can take measures to reduce the impact of the Personal Data Breach).

REPORTING TO THE BOARD OF TRUSTEES

11.26 The Data Protection Officer shall be responsible for notifying the Audit and Risk Committee of the number of breaches occurring and of any specific aspects of the breach which require notification due to the seriousness of the breach or specific circumstances relating to the breach which the Audit and Risk Committee should be aware of (such as poor practice, recurring issues, individual actions, involvement of a major third party contractor and a services near-miss etc).

REVIEWING THE RESPONSE

11.27 Once the Personal Data Breach has been dealt with, we will consider and evaluate the response. Consideration should be given to:

- the speed of the response;
- the adequacy of the response;
- whether any further training is required for staff;
- whether any procedures or processes need to be amended; and
- whether any current policies should be amended in light of the Personal Data Breach.

11.28 If applicable, the results of any review should be communicated to members of staff.

12. RIGHTS OF A DATA SUBJECT

12.1 We must put in place processes to enable Data Subjects to exercise their legal rights.

12.2 A Data Subject has the following rights under the UK GDPR:

- A right of access to their personal data and certain other information;
- A right to have any personal data which we hold which is inaccurate rectified;
- A right to have incomplete personal data completed;
- In certain circumstances, a right to have personal data concerning them erased;
- In certain circumstances, a right for the processing of their personal data to be restricted;
- In certain circumstances, the right to receive the personal data that the Data Subject has provided him or herself, in a portable format that can be transmitted to another controller;
- The right to object to certain types of processing, including profiling and processing for direct marketing purposes; and
- In certain circumstances, the right not to be subject to a decision which is based solely on automated processing.

12.3 We must provide information requested by a Data Subject under the UK GDPR without undue delay and, in any event, within one month of receipt of a request. This period may be extended by a further two months, if for example there are a number of requests made or a request is particularly complex. Therefore, if you receive a request from a Data Subject concerning their personal data, please notify the Data Protection Officer immediately.

12.4 As stated in Section 2.40, as an Academy Trust we are not covered by the Educational (Pupil Information) (England) Regulations 2005 in respect of access to a pupil or student's educational record. Please see Section 2.40 for further information in this regard.

12.5 As part of our work with pupils, students and staff, we may process information, such as confidential references, exam scripts, details of social work activity, child protection issues, SEN information and adoption records. Specific protections are in place in respect of these types of information, which mean that they may be exempt from disclosure as part of a subject access request. If you receive a request for these types of information, please follow the third-party requests for data procedure outlined below and contact DPO@deltatrust.org.uk.

12.6 The Trust's Subject Access Request form is attached as **Appendix 2** to this policy.

12.7 The Data Protection Officer shall maintain a record of all Data Subject rights requests. This record will contain at least the following information:

- the Applicant;
- if the Applicant is someone other than the Data Subject, the name and relationship with the Data Subject;
- the date of the request;
- the Data Subject right being exercised (the right to be forgotten, the right of erasure or Data Subject access right etc.);
- the date the request was completed; and
- a general description of the information requested.

13. THIRD PARTY REQUESTS FOR DATA

13.1 If we receive a request from someone other than the Data Subject or someone acting on their behalf, we must first establish the authority requesting the information has the right to such information. The Data Protection Legislation allows the Police and other authorities such as the Department for Work and Pensions Benefit Fraud section, which have powers to prosecute, to gather data from organisations, which is unavailable elsewhere, such as the address and contact details of employees and ex-employees subject to certain restrictions.

13.2 This may include where the information is required for matters relating to national security, national defence, public security, the prevention, investigation, detection or prosecution of criminal offences. Such rights are often used to gain access to the address and contact details of employees and students and ex-employees and students. If in doubt, you should ask the authority to quote the piece of legislation they are relying on for you to provide the information to them.

13.3 In such cases, an exemption included in the Data Protection Legislation may apply and allow us to share information without an individual's consent, in certain circumstances. These circumstances include:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty.

13.4 In these cases, we will document any decisions we have taken regarding the sharing of personal data without the individual's knowledge, including the reasons for those decisions.

13.5 Sometimes the Police and other authorities may write or call the organisation in circumstances where there is not a strict legal requirement to provide the information to them. In such circumstances it is important we understand the limitations of such requests as they do not create an automatic requirement on us to provide the information.

13.6 Where we are required to provide information to the Police or other authorities in certain circumstances (such as when it relates to the investigation of crime) Data Protection Laws exempt us from various requirements, such as the obligation to tell individuals their data is being processed, as this could, for example, notify them that they are being investigated.

13.7 However, even if Data Protection Legislation allow us to provide information to the police or other authorities, we still need a valid processing condition in place. If the data requested includes special category personal data, the circumstances in which it can be released will be more limited. Relevant processing conditions under Data Protection Legislation may include where it is pursuant to a legal obligation (such as where there is statutory obligation to assist in an investigation) or where the prosecuting authority has a warrant. Where this is the case, the information must be provided.

13.8 In the event that any request is made for information by a third party, please contact the Data Protection Officer via DPO@deltatrust.org.uk.

13.9 When considering requests, we must:

- ensure that we properly identify the person requesting the information. If the request is made by phone, ask for a written request to be submitted from an official email address or on official letter headed paper.
- if there is no warrant or legal obligation to provide the information, we must consider whether a refusal to provide the information requested will impede the investigation; and
- provide the minimum information required to fulfil the request (unless the circumstances of the investigation justify greater disclosure (such as in a serious criminal investigation (particularly where there is a real danger to the public or an individual)).

13.10 If a third party seeks information under the UK GDPR, the Data Protection Officer must be consulted, who will verify whether or not such request needs to be complied with.

14. DATA RETENTION

14.1 We shall retain all Personal Data in accordance with our Trust Personal Data Retention Policy and in any event for the minimum periods required by law. Certain documents such as accounting, tax and employment records have

specific retention periods. The destruction of other records may, in the context of litigation, be regarded unfavourably by the courts.

14.2 We shall arrange for all personal data records to be regularly reviewed to ensure that they are accurate, not excessive, up to date and adequate for their purposes. If we believe that any Personal Data we hold is inaccurate and/or not-up-to date, we shall notify the relevant person and request that they confirm their accurate and up-to-date details.

14.3 The Personal Data we hold shall be kept for at least the minimum periods set out in the Trust Personal Data Retention Policy. Information may be kept longer than these minimum periods at the discretion of the Data Protection Officer where retention can be justified, provided that such personal data is not kept longer than is necessary for the purpose for which the data was collected.

14.4 Where documents are destroyed pursuant to the time periods set out in the Trust Personal Data Retention Policy, we shall follow the procedure for destruction set out in Section 10.32.

15. USE OF VIDEO SURVEILLANCE EQUIPMENT

15.1 Video surveillance systems process personal data through the use of CCTV and ANPR. The processing of personal data using video surveillance equipment is intrusive by its nature and where public areas are monitored using such video surveillance equipment, specific concerns may be raised under the Data Protection Legislation. We will ensure that all data recorded by such systems is processed in accordance with this policy.

15.2 We will keep a record of all video surveillance systems we operate. The record will contain:

- what cameras are kept and where;
- the purpose of the video surveillance system. This should include an assessment of the process and the reasons for installation of the scheme; and
- confirmation that all video surveillance systems are accounted for in our ICO notification.

15.3 Where possible, all video surveillance systems should be sited so that they only record that information which is necessary for the purpose of the scheme (i.e. for example, CCTV systems should not capture images of people visiting adjacent premises). Care should be taken to ensure that images are not taken of public or domestic areas, or if they are, that this is restricted in so far as possible. We shall carry out a data privacy impact assessment for all new video surveillance systems (and for any material changes to such systems). Where an outside contractor is used for the operation of the video surveillance equipment, the Trust shall carry out due diligence to ensure the contractor has the appropriate skills, experience and equipment to conduct such surveillance and, where necessary, that they have the appropriate licensing in place.

15.4 Video surveillance systems should only be accessed and operated by specified individuals who have been trained appropriately. In academies this will be the Principal/Head of Academy or a designated member of staff. At Head Office, this is the Facilities Manager or the ICT Management Team. Video surveillance images contain personal data and should only be processed by the Trust in accordance with the Data Protection Legislation. Video surveillance images must not be copied or circulated within the Trust unless the Data Protection Officer or CEO has provided written permission. In the event that any transfer is authorized, this must be by secure means, following advice provided by the Trust's ICT Team.

15.5 All video surveillance installations should be located in a secure environment e.g. a locked server room or Facilities Office.

15.6 Access to all images should be password protected and no remote access or monitoring should take place by either third parties or academy staff without authorisation from the Director of ICT.

15.7 All zones covered by video surveillance equipment should have signs displayed indicating that individuals are entering a video surveillance zone. Such signs should be visible and legible.

15.8 The signs should:

- include our name;
- include the purpose of the scheme (see below);
- include who to contact about the scheme; and
- be an appropriate size depending on the context, for example, whether they are viewed from a distance.

For example, a sign could say "Images are monitored in order to provide a safe and secure environment for students, staff and visitors, as well as to protect academy property, crime prevention and public safety. Please contact [ ] on [insert telephone number] for more information".

15.9 Video surveillance equipment must not be used for covert surveillance without the permission of the Data Protection Officer. Covert surveillance must only be used where there is clear evidence of illegal activity taking place and after consultation with the Police, if necessary, or other relevant enforcement bodies. Covert surveillance of children is particularly sensitive and would be difficult to justify in all but the most serious cases.

15.10 Images captured by video surveillance systems must not be retained longer than necessary. Images will be retained for a maximum of 45 days before being recorded over, unless exceptional circumstances apply and the Trust's Data Protection Officer has approved this extension.

15.11 If a subject access request is received, consideration should be given as to whether images of third parties also included should be obscured. This will be necessary if providing the image would unfairly intrude on the third party's privacy.

15.12 Except for law enforcement bodies and pursuant to subject access requests, video surveillance images or remote external access to them should not be provided to third parties, unless this has been agreed in advance by the Data Protection Officer.

15.13 We will check the system regularly to ensure no fault develops or the image quality decreases. At least annually, Academy staff must evidence their review of the system.

15.14 If we are considering using an existing video surveillance system for a new purpose, or we make a material change to the system, we must carry out a data protection impact assessment.

16. USE OF BIOMETRIC SYSTEMS

16.1 Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements.

16.2 The Information Commissioner considers all biometric information to be personal data as defined by the Data Protection Legislation; this means that it must be obtained, used and stored in accordance with Data Protection Legislation.

16.3 The Protection of Freedoms Act 2012 includes provisions which relate to the use of biometric data in schools and colleges when used as part of an automated biometric recognition system. These provisions are in addition to the requirements of the Data Protection Legislation.

16.4 'Processing' of biometric information includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data including (but not limited to) disclosing it, deleting it, organising it or altering it. An automated biometric recognition system processes data when:

- recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;
- storing students' biometric information on a database system; or
- using that data as part of an electronic process, for example, by comparing it with biometric information stored on a database in order to identify or recognise students.

16.5 Academies must ensure that the parent/person with parental responsibility of each child is informed of the intention to use the child's biometric data as part of an automated biometric recognition system. In **no** circumstances can a child's biometric data be processed without written consent.

16.6 Academies must not process the biometric data of a student where:

- The child (whether verbally or non-verbally) objects or refuses to participate in the processing of their biometric data;

- A parent, someone with parental responsibility or student has not consented in writing to the processing; or
- A parent, someone with parental responsibility or student has objected in writing to such processing, even if another parent has given written consent.

16.7 Academies must provide reasonable alternative means of accessing the services to those students who do not want to use an automated biometric recognition system. In most cases this will take the form of a PIN number.

16.8 The original written consent is valid until such time as it is withdrawn. However, it can be overridden, at any time either parent/person with parental responsibility or the child themselves objects to the processing (subject to the parent's objection being in writing). When the student leaves the academy, their biometric data will be securely removed from the academy's biometric recognition system.

17. HOME WORKING AND WORKING AWAY FROM THE OFFICE

17.1 During the course of your employment, there may be times when you will work away from our offices either at home or whilst travelling ("**Home Working**"). In addition to agreed line manager approval requirements, you must seek permission to work from home unless you are doing so with a Trust laptop or mobile device. Where you seek permission to work from home, in addition to Line Manager approval, we will need to consider the following issues:

- information handling - this includes handling data on home pc's, laptops, tablets, smart phones, mobile devices and removable media as well as paper files:
- use of services - remote access to our IT system and services: and
- systems - managing personal computers and other devices (e.g. to ensure that viruses are not introduced).

17.2 Use of our facilities (e.g. laptops and remote services) when Home Working is for your own work-related use, and such facilities are provided only for authorised purposes. You have a responsibility to ensure that other people do not have access to our systems, facilities and services, confidential information, personal data or sensitive personal data (the "**Information**").

17.3 Any loss of information must be reported in accordance with the Personal Data Breach section of this policy.

17.4 You must keep all information secure when in transit between locations. For example, never leave a laptop or work papers unattended in a public place. When you have finished work, you should shut down your computer or laptop and put away any papers you have used in a secure place, even if you are at home. When travelling with a laptop, keep it in your hand luggage.

17.5 You should avoid taking Information home whenever possible. Where this cannot be avoided, you should adopt security measures appropriate to the nature of the data.

17.6 In order to ensure compliance with the six data protection principles, you should keep work related information and files separate from your personal files and when the Information is in paper form, preferably in a lockable filing cabinet. Where possible, work from home should be carried out in a designated area in your home. For example, where you live in a home with individuals who are not members of your family or children, you should avoid working in a communal part of your home such as a lounge or kitchen.

18. BRING YOUR OWN DEVICE (BYOD)

18.1 This applies to the use of smartphones, mobile phones, PDAs, tablets, laptop or notebook computers including any accompanying software or hardware ("**Device**") for business purposes. You must not use your own Device for work purposes except as set out in this section. This section applies to use of the Device both during and outside office hours and whether or not you use the Device at your normal place of work.

18.2 Access to the corporate network and associated data systems is centrally managed by the ICT Department. Requests for access must be submitted to the ICT department via the ICT service desk.

18.3 We reserve the right to refuse or remove permission for your Device to connect to our systems. The ICT Department will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a Device is being or could be used in a way that puts, or could put, us, our staff, our business connections, our systems, or our corporate information at risk or that may otherwise breach this policy.

18.4 In order to access our systems, it may be necessary for the ICT Department to install software applications on your Device. If you remove any such software, your access to our systems will be disabled.

18.5 All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a Device (collectively referred to as ("**content**") in this policy) during the course of business or on our behalf is our property insofar as it is created by us or on our behalf, regardless of who owns the Device.

18.6 We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire Device (including personal content) for litigation or investigations.

18.7 You must comply with our Trust Online Safety Policy when using your Device to connect to our systems.

18.8 In the event of a lost or stolen Device, or where a staff member believes that a Device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report this to the Data Protection Lead and log an incident with the ICT Team immediately.

18.9 On your last day of work, or your last day before commencing a period of garden leave, all data relating to the Trust (including work e-mails), and any software applications provided by us for business purposes, will be removed from the Device. If this cannot be achieved remotely, the Device must be submitted to the ICT Department for wiping and software removal. You must provide all necessary co-operation and assistance in relation to this process. If you do not provide the Device to us and it can be wiped remotely, we reserve the right to remotely wipe it and remove software.

18.10 We do not provide technical support for Devices. If you use a Device for business purposes you are responsible for any repairs, maintenance or replacement costs and services.

18.11 You must pay for your own Device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By using a Device for business purposes, you acknowledge that you understand that your business usage of the Device may increase your voice and data usage charges.

APPENDIX 1 – DEFINITION OF DATA PROTECTION TERMS

The following terms are used throughout this policy. It is important that you understand their meaning. Many of the terms are set out in the Data Protection Legislation.

Term	Definition
"**Data**"	is information which is stored electronically, on a computer, or in certain paper-based filing systems. The Data Protection Legislation is not restricted to information held on computers. Electronic data includes data kept on computer and other digital devices such as laptops, tablets, smart phones, mobile phones and digital cameras. Paper based filing systems such as an HR filing cabinet, with employees listed alphabetically, a diary, or student files listed alphabetically, will be covered by the Data Protection Legislation.
"**Data Subjects**"	for the purpose of this policy includes all living individuals about whom we hold personal data. A Data Subject does not need to be a UK national or resident. All Data Subjects have legal rights in relation to their personal data.
"**Personal Data**"	means any information about an identified or identifiable individual who can be identified: • from that data; or • from that data and other information which is in the possession of or is likely to come into the possession of the data controller; or • directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of an individual. Personal data includes any expression of opinion about an individual and any indication of the intentions of the controller or any other person in respect of the individual. Note, the definition does not cover companies (although it does cover individuals within companies) nor does it cover information about the deceased.
"**Personal Data Breach**"	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
" **Controllers**"	are the people who, or organisations which, determine the purposes for which, and the manner in which,

Term	Definition
	personal data is processed. They have a responsibility to establish practices and policies in line with the Data Protection Legislation.
" **Processors**"	include any person who processes personal data on behalf of a controller. Employees of controllers are excluded from this definition but it could include suppliers which handle personal data on behalf of the Trust
"**Processing**"	is any activity that involves use of the data. You (and therefore we) will process personal data when you obtain, record or hold the data, or carry out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
"**Special category personal data**"	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (such as data relating to the inherited or acquired genetic characteristics of an individual), biometric data (for the purpose of uniquely identifying an individual), data concerning an individual's health (including both physical and mental health), sex life or sexual orientation. Special categories of personal data can only be processed under strict conditions and will usually require the express consent of the person concerned. Criminal data is not included within the definition of special category data but we should process criminal offence and conviction data using the same safeguards we operate with in respect of special category data.

APPENDIX 2 – SUBJECT ACCESS REQUEST FORM

Are you employed by the Trust? Yes No

If you are employed by the Trust what position do you hold?

_____

Please provide the details of the person requesting the information:

Full Name: _____

Address: _____

Telephone Number: _____

Email: _____

Are you the Data Subject? Yes No

If you are the Data Subject, please provide the following:

driving licence or passport or other document showing name and signature;

a recent bill (e.g. credit card bill, bank statement or utility bill) or insurance document showing name and address; and

a stamped, addressed envelope for return of proof of authority documents.

If you are not the Data Subject, please provide full details of you and the Data Subject:

Data Subject Name: _____

Your Full Name: _____

Address: _____

Telephone Number: _____

Email: _____

If you are not the Data Subject, please provide:

proof that the Data Subject has authorised you to request data on their behalf. A signed letter authorising you to act on behalf of the Data Subject will be sufficient;

if you have parental responsibility for a pupil /student and you are asking for information about that pupil / student:

- if the pupil / student is aged 13 or over and we deem that a pupil / student is able to understand the nature of, and make a subject access

request, proof that the pupil / student has authorised you to request data on their behalf (see 7.1); or

- if the pupil / student is under 13 (or is aged 13 or over but we deem that that pupil / student is not able to understand the nature of, and make a subject access request), please provide:
    - evidence of your identity; and
    - if requested, evidence that you have parental responsibility for that pupil / student; and

a stamped, addressed envelope for return of proof of authority documents.

Scope of Request

Please provide a description of the personal data you are requesting and any information you have as to the location of the data. For example, the department, school or office of the Trust relevant to your request.

_____

_____

_____

Locating the Personal Data

If you would like a more general search, please note that we would normally search our supplier database if you are a supplier and our Finance Office, Personnel Files and Payroll Department if you are an employee of the Trust. If there are any other files which you believe we should search, please advise.

_____

_____

_____

Declaration

I certify that the information given on this Subject Access Request form is true and that the Trust may contact me in order to obtain further details about the information requested if this is required.

Signed: _____

Full name: _____

Date: _____

Where to send your request

Please send this completed form to Data Protection Officer, Delta Academies Trust at Education House, Spawd Bone Lane, Knottingley, WF11 0EP.

When will I receive a response?

A response will be sent to you within the statutory time limit of one calendar month.

APPENDIX 2 – SUBJECT ACCESS REQUEST FORM - NOTES ON DEALING WITH DATA SUBJECT ACCESS REQUESTS

What is a Data Subject Access Request?

1. Data Subjects have a right of access to a copy of their personal data and certain other information.

2. A subject access request is any written request from a Data Subject, which indicates that the person wants to know what information is kept about them.

3. If a verbal request for information is received you should ask the Data Subject to put the request in writing, but should still treat the verbal request as a valid request. The time for us to respond to such a request commences once the verbal request has been made.

4. If you receive a verbal request and have reasonable doubts as to the identity of the person making the request, we may request additional information to confirm the identity of the requester before responding to their request.

5. Internal Data Subject access requests will be treated as being of equal importance to external data subject access requests.

6. Answering a subject access request can be time consuming. We will ensure we have adequate resources available to answer subject access requests that are made.

What should I do if I receive a Data Subject Access Request?

7. You must pass all Data Subject access requests to the Data Protection Officer via DPO@deltatrust.org.uk for processing as soon as possible, as a response must be given within one month. Any delay in passing the request to the Data Protection Officer could result in us failing to meet the statutory deadline and result in enforcement action by the ICO.

Responding to a Data Subject Access Request

8. It is the Trust's responsibility to respond to a Data Subject access request. You must not send a response without consulting the Trust via DPO@deltatrust.org.uk.

9. Data Subject access requests must be complied with promptly, and in any event, within one calendar month of the receipt of the request. The period to respond may be extended by a further two months, if the request is complex and/or there are a number of requests.

10. We are entitled to ask the Data Subject for further information to help us find the data requested. For example, we could ask for the dates an employee was employed by us or at which site they worked. The calendar month period does not start until this additional information is received.

11. Information provided in response to a subject access request should be free of charge, unless we can demonstrate that the request is manifestly unfounded

or excessive (e.g. the requester has made repeated requests for information). In these cases, we can charge a reasonable fee to cover our administrative costs of providing such information and taking the action required, or, alternatively, we can refuse to provide the information.

12. When a written Data Subject access request is received, the individual should:

- be told whether we or a third party is processing the individual's personal data.
- be provided access to the personal data;
- be given a description of:
  - the personal data;
  - the purposes for which it is being processed;
  - the categories of personal data concerned e.g. employer/ pupils and students/ parents and guardians;
  - those people and organisations to whom the personal data may be disclosed (including any countries outside the UK);
  - where possible, the period it is envisaged that the personal data will be stored for, or if this is not possible, the criteria used to determine that period;
  - their right to request rectification, erasure or the restriction of the processing of their personal data, or to object to such processing;
  - the right to lodge a complaint with the ICO;
- where the data has not been collected from the Data Subject, any available information as to where it was sourced from;
- the existence of automated decision making (including profiling), including meaningful information about the logic involved, and the significance and envisaged consequences of such processing to the Data Subject; and
- be provided with a copy of the information.

13. We must provide a copy of an individual's personal data that is undergoing processing. If an individual requests more than one copy of their information, we may charge a reasonable fee based on our administrative costs incurred in dealing with such a request.

14. Where a Data Subject makes a subject access request via written or electronic means, then unless they request otherwise, we shall provide any information to them via recorded delivery post.

15. In responding to Data Subject access requests, we are required to ensure information relating to an individual, other than the Data Subject who is making the request, is not disclosed unless:

- the other individual has consented to such disclosure, in which case written proof of this should be obtained and kept; or
- it is reasonable in all the circumstances to comply with such request without any consent. This may be the case if the information is already available to the public, for example.

16. In considering whether it is reasonable to comply with the request, we will consider:

- any confidentiality owed to the other individual either because we said this information would be kept confidential, or because of the particular circumstances it was disclosed in, or because of the nature of the information;
- the steps taken to get consent;
- if the individual concerned can give consent; and
- any express refusal by such individual to give consent.

17. A subject access request entitles the Data Subject to information, which contains their personal data. It does not entitle the Data Subject to all word documents, e-mails etc. which they were copied in on, or which relate to work or projects they were involved in. Where a document contains personal data but also information about other third parties which should not be disclosed, or contains information which is not personal data, then the document can be provided to the applicant with the information which is not their personal data redacted (blacked out) in the document.

18. All personal data shall be stored at all times by employees in paper and electronic filing systems owned and/or operated by the Trust which enable us to provide a Data Subject with details of such personal data promptly and in any event within the time period provided for by the Data Protection Legislation.

Requests for access to special categories of personal data

19. All requests by external bodies, agencies or individuals for access to special categories of personal data shall be processed by the Data Protection Officer.

20. All such requests shall be recorded by such persons in an appropriate system.

21. The record should state who made the request, when they made it, what the request was and to whom it related.

Requests for pupil / student data

22. When a request for pupil / student data is made (including any pupil's / student's sensitive data), then in addition to the steps identified above, we must also ensure that we comply with the following steps before responding to any request for pupil / student data:

    a) Ensure that the necessary consent has been obtained. This means that you must be satisfied that:

        - If the request is received from the pupil / student directly, that they understand the nature of the request that they have made. Each pupil / student and the level of their understanding must be judged on a case-by-case basis, but, if a pupil / student is aged 13 or over, then we will assume that they have the competence to understand and make a subject access request, subject to the completion of an assessment of their competency.

- If the request for pupil / student personal data is received from someone with parental responsibility for that pupil / student, then you must be satisfied that either:
    - the pupil / student is too young to consent (if a child is under 13 years of age they will generally be considered to not have competence); or
    - the pupil / student is aged 13 or over and you are satisfied that the pupil / student has consented to the disclosure of his/her personal data and this consent has been demonstrated to the Trust (e.g. a signed letter from the pupil / student, or if he/she confirms to the Trust in person).

b) If a subject access request does not come from the pupil / student (other than from someone with parental responsibility for them, if that pupil / student is under 13 years of age), then we must not disclose any personal data until we are satisfied that the pupil / student has consented to the disclosure of his / her personal data, as the person making the subject access request is, in effect, exercising the pupil's / student's right of subject access on that pupil's / student's behalf.

- If an objection to disclosure is made by a pupil / student who is deemed to be sufficiently mature and aware, then this must be respected.
- We must also be satisfied, before any disclosure of a pupil's / student's personal data is made, that the recipient of such personal data, if it is not to the pupil / student directly, is in fact a person with parental responsibility for that pupil / student. **If you have any doubt about the identity of the person making the subject access request, then you must ensure that you have evidence of their identity before any disclosure is made**.

23. If a subject access request is made for pupil / student personal data, the exemptions contained within the Data Protection Legislation, provide that certain information may not need to be disclosed as part of a subject access request.

24. If you have any queries on whether any student personal data may be exempt from disclosure under the Data Protection Legislation, or any other statutory provisions, then you must contact the Data Protection Officer.

APPENDIX 3 -DATA SECURITY BREACH INCIDENT FORM

PART 1

Name of Reporter: _____

Date of Notification:

_____

Date of Incident: _____

General Description

1. Describe the incident in general terms. You should include the information disclosed, an outline of the number of records and/or Data Subjects affected and a general description of how the incident occurred. This should be outline information only. The sections below will guide you through the detailed information we require.

_____

_____

_____

_____

_____

_____

Details of Incident

2. Detail when the incident occurred and, if available, attach any documentation relating to the incident

_____

_____

_____

_____

_____

_____

3. Provide a summary of the incident and the background to the incident. How did the incident occur? Why and/or how was the data lost or misused?

Details of the Data

4. Describe the format of the data (for example, a paper file or electronic document)

5. Detail the number of records and Data Subjects affected and how

6. Describe the nature of the data (for example, addresses, bank account details, National Insurance numbers)

Other details

7. Detail the possible and actual harm to the Data Subjects

8. Detail the number of complaints and attach copies of these

9. State whether a data processor or sub-processor was involved. If so, provide the name of the processor and, if you have access to it, a copy of the contract entered into between the Trust and the processor

PART 2 – To be completed by the Data Protection Officer

Date completed: _____

Date ICO informed (if applicable): _____

Processor

1. If a processor or sub-processor was involved, was the data protection provisions within the contract entered into between the Trust and the processor breached and what are the possible contractual remedies available

_____

_____

_____

_____

_____

_____

Investigation

2. Describe the investigation and, where possible, provide the following information:

Members of the incident response team and lead officer

Which of the following actions were taken to contain the incident:

- Notification of legal counsel
- Notification of Data Subjects or anyone with parental responsibility for them
- Notification of key internal stakeholders (for example, senior management or the board of Trustees)
- Notification to ICO
- Consideration of the likelihood of media interest and, if applicable, the preparation of talking points/consultation with PR company

Assessment of Response and Suitability of Procedures

3. Detail any action taken to ensure there is no repeat of the same incident. Determine:

3.1. How well the Trust reacted to the incident

_____

_____

3.2. Whether documented procedures were followed and, if so, whether they worked

_____

_____

3.3. What could have been done differently

_____

_____

3.4. Whether there is a need to update procedures

_____

_____

3.5. Whether there is a need to reassess organisational, physical or technical security

_____

_____

3.6. Whether any of the following issues need to be reassessed:

- risk assessment/privacy impact assessments for new activities involving personal data

_____

- allocation of responsibility of data protection

_____

- training for relevant staff in the Trust's responsibilities and how to meet them

_____

- awareness raising of data protection issues

_____

APPENDIX 3 – DATA SECURITY BREACH INCIDENT FORM - NOTES ON COMPLETION

Notes for completion

What information is required when reporting a Personal Data Breach to the ICO?

In order to ensure that we can deal with the Personal Data Breach in the appropriate manner, it is important that accurate and complete information about the breach is provided to us.

1. You should fill in Part 1 of the Security Breach Incident Form set out above and pass the completed form to the Data Protection Officer, without delay.

2. You need to try to remember or describe, to the best of your knowledge, the circumstances of the Personal Data Breach, including:

    - the quantity of data concerned;
    - the nature of the data,
    - the categories of Data Subjects (e.g. pupils/parents and guardians/employees),
    - whether or not the information lost or destroyed or wrongly processed is special category personal data, high risk data or is particularly important.

3. Special category personal data is defined in Appendix 1.

4. High risk data includes data relating to identity theft or fraud including bank account details, passport numbers, driving licence details and national insurance numbers.

5. You should tell us the likely consequences of the breach and a description of the methods you have taken to deal with the breach.

6. The surrounding circumstances as to how the breach occurred may be very important. You should consider the following and be ready to provide this information to the Data Protection Officer when reporting the breach:

    - when the Personal Data Breach occurred (this will be particularly relevant if the Personal Data Breach involves illegal activity);
    - how the data was stored including any relevant security measures relating to the method of storage (for example, paper records in a file or electronic records on a laptop);
    - who was responsible for the data at the time of the Personal Data Breach;
    - whether a third-party processor was involved; and

- how the Personal Data Breach occurred (for example, was the data misplaced or stolen).

7. If a third-party processor is involved in processing any personal data which forms part of the Personal Data Breach, that processor should be asked to provide all reasonable assistance and cooperation in dealing with and remedying any Personal Data Breach. Under the UK GDPR they have a legal obligation to assist.

Notifying the Personal Data Breach to individuals affected by the breach and others

8. Under the UK GDPR there is a statutory obligation on us to notify affected individuals where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of those individuals.

9. A high risk will occur where the data breach relates to high risk data

10. We will notify individuals whose data is involved in the Personal Data Breach in order to allow them to take any necessary steps to mitigate their losses. The Data Protection Officer shall decide whether any individuals should be notified of the Personal Data Breach. However, please be aware that the ICO can require us to notify individuals if we have failed to do so, but it believes the Personal Data Breach creates a high risk.

11. In addition to notifying individuals, we will consider notifying the following parties of the Personal Data Breach:

    - outside media;

    - the police if the Personal Data Breach has arisen as a result of illegal behaviour such as theft, hacking or a denial of service attack; and

    - other affected parties.

12. Any decision to notify affected individuals will be based on the requirements of the UK GDPR, ICO guidance, whether the Personal Data Breach is likely to result in a high risk to that individual and whether or not notification will assist the individual to mitigate his/her loss arising out of the incident. If an individual is notified of a Personal Data Breach, we must notify them without undue delay. We must also notify the Personal Data Breach to an individual if required to do so by the ICO.

Assessing the risk

13. Once notified of a potential Personal Data Breach, the Data Protection Officer may appoint a team of individuals to investigate the incident. The team is responsible for assessing the risk level of the Personal Data Breach incident and assessing the adverse consequences of the Personal Data Breach to the individuals involved.

14. Determining whether or not the breach is a risk requires consideration of the likelihood and severity of the risk caused by the data security breach to individuals. When you consider the risk you should take into account:

- the type of breach;
- the nature, sensitivity and volume of personal data;
- ease of identification of individuals;
- the severity of consequences for individuals;
- special characteristics of the Data Subjects affected; and
- the number of affected individuals.

15. Part of the classification of the risk is also dependent on our own characteristics as a controller. As the Trust operates in the education sector there is an inherent risk in our processing activities which should be taken into account in any decision as to whether or not the breach presents a risk or a high risk.

16. It is more likely a breach will be considered to be high risk where it may lead to physical, material or non-material damage. This would include discrimination, identity theft or fraud, financial loss and damage to reputation. Where the breach involves special category data, criminal convictions data or related security measures, it is much more likely to be regarded as high risk.

Containment and recovery

17. Consideration should be given as to whether there is anything that can be done to mitigate the loss (for example, whether any of the data can be recovered).

18. We will appoint a team of individuals to work on containing the Personal Data Breach if applicable. The team should be given clear instructions as to what their tasks are (for example, they may be instructed to close a weakness in the IT system through which data has been released).

19. Consideration should be given as to whether there is anything we can do to limit the damage (for example, utilising back up records to restore the data that is the subject of the Personal Data Breach or promptly notifying individuals affected so they can take measures to reduce the impact of the Personal Data Breach).

APPENDIX 4 – CONSENT FORM

CONSENT FORM (PUPIL PERSONAL DATA)

During your /a pupil's time with us we will gather information about you/them which we will use for various purposes. A Privacy Notice has been provided to you/them in relation to the use of this information, which is also available on the school website.

There are some things that we cannot do unless you tell us that we can. We have set these out in the tables attached. Please could you read this form carefully and tick the appropriate options. This will let us know which of these things you are happy for us to do, and which you are not.

You can refuse to provide your consent to the items listed overleaf. You do not have to provide reasons for this and it will not affect your /your child's place at the Academy. If you wish to provide additional information, we will use this to understand any concerns that you have and take appropriate steps, where necessary.

Photographs and Videos

Some of the information in the attached tables includes photographs and videos of you /your child. We have a number of measures in place to mitigate against the potential misuse of photographs and videos of our pupils/ students. These include:

- The Trust Online Safety Policy and Procedure provides guidance to staff on the capture, storage and publication of images.
- Students/Parents/Carers may withdraw permission, in writing, at any time.
- Students' full names will not be published alongside their image.
- Email and postal addresses of students will not be published.
- Before posting student work on the Internet, a check is made to ensure that permission has been given for work to be displayed.
- No photos will be uploaded to a website or published, without prior checking with the Head of Academy /Principal or nominated responsible person at the Academy.

Please note that the Academy or Trust may provide photographs and videos to the media, or be visited by the media who may take videos and photographs. The Academy or Trust does not have control over these images once this has taken place.

Celebrating Your /Your Child's Achievements and Reporting on Events
As an Academy and a Trust, we are very proud of the achievements of our pupils/students and we would like to be able to celebrate these achievements both within the Academy and Trust and with others. We may also want to report on significant events which involve our pupils, such as visits from dignitaries. This will involve providing information about involvement in certain activities.

	YES (✓)
In order to celebrate my /my child's achievements, I consent for the Academy/the Trust to use:	
Photographs of me /my child	
Videos of me /my child	
My /my child's first name	

	YES (✓)
I consent for the information selected above to be used:	
In the Academy on notice boards and screens	
On the Academy/Trust website	
On the Academy/Trust social media sites (e.g. Twitter)	
In the media – newspapers, websites and television	

Promoting the Academy and the Trust
We would like to be able to promote the Academy and the Trust to attract new pupils, to recruit new staff and to show the great opportunities provided to our pupils, students and staff. As part of this we would like to be able to use photographs and videos of our pupils and students in promotional material. This will include our prospectus, on our websites, on social media and where appropriate, may include taking part in local and national media opportunities.

	YES (✓)
I consent for the information selected below to be used for the purpose of promoting the Academy/Trust: **Photographs of me /my child**	
Videos of me /my child]	
My /my child's first name	

	YES (✓)
I consent for the information selected above to be used: **In Academy/Trust publications (e.g. Prospectus, Recruitment)**	
On the Academy/Trust website	
On the Academy/Trust social media sites (e.g. Twitter)	
In the media – newspapers, websites and television	

You may change your mind in relation to any of the consents that you have provided at any time. This includes withdrawing your consent to anything that you have agreed to here.

To withdraw your consent to any of the above, or otherwise amend your position, please write to us at:

School Office [INSERT SCHOOL DATA LEAD CONTACT DETAILS]

This consent will otherwise continue until you /your child leaves the Academy (or your child reaches the age of 13 years old at which point the Academy will seek consent directly from your child in relation to the above matters).

Pupil/Student name: _____

Date of birth:

_____

Tutor group: _____

Signed: _____

Name: _____

Relationship to pupil/student:

_____

Date: _____

APPENDIX 5 – DATA PROTECTION COMPLAINT FORM

1. What is your relationship with the Trust (e.g. employee, pupil / student, supplier)?

   _____

2. If you are employed by the Trust what position do you hold?

   _____

   _____

3. Does your complaint relate to a Subject Access Request/exercise of Data Subject rights?

   Yes No

4. If your complaint relates to a Subject Access Request or the exercise of any data subject right (such as the right to be forgotten, or the right to restrict), please confirm the date of your request and the Data Subject it concerned. If you have the SAR or other Data Subject request reference number, please provide this below.

   _____

5. If your complaint follows correspondence with an employee of the Trust, please state the employee's name and the date(s) of your correspondence

   _____

6. Describe the incident(s) prompting your complaint (for example, if your complaint is regarding the misuse of data, you should describe the data, the reason the data was provided to the Trust and how you believe the data has been used incorrectly)

   _____

   _____

   _____

   _____

   _____

7. If you have any documents which help detail your complaint, such as copies of correspondence with the Trust or an individual employee, please attach these to the form and detail below. Please only send documents which are directly relevant to your complaint

_____

_____

_____

8. What is your desired outcome of this complaint (for example, the correction of inaccurate data)?

_____

_____

_____

_____

9. Please provide the following contact details:

Address: _____

Telephone Number: _____

Email: _____

Declaration

I certify that the information given on this complaints form is true and that the Trust may contact me in order to obtain further details, if required, or provide a substantive response.

Signed: _____

Full name: _____

Date: _____

Where to send your complaint

Please send this completed form for the attention of the Data Protection Officer to Delta Academies Trust, Education House, Spawd Bone Lane, Knottingley, WF11 0EP.

When will I receive a response?

A substantive response will be sent to you within 28 days.

APPENDIX 6 – PRIVACY NOTICES: HOW WE USE PUPIL INFORMATION

As your school we need to use information about you. We do this for a number of reasons. This form tells you what information we use about you and why we use it. It is very important that information about you is kept safe. We explain below how the school keeps your information safe.

If you want to know anything about what we do with information about you, then please ask your teacher, or speak to your parent/carer and ask them to contact the Academy. We also have a person called the Data Protection Officer who works with your Academy. They can answer questions you have about what the school does with your information. If you or your parent/carer want to speak to them, then you can contact them via: DPO@deltatrust.org.uk.

Policy Statement

During your time with us, we will use information that we gather in relation to you for various purposes.

Information that we hold in relation to you is known as "personal data".

This will include data that we obtain from you directly and data about you which we obtain from other people and organisations.

We might also need to continue to hold your personal data for a period of time after you have left the school.

Anything that we do with your personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we use about you?

We will collect, hold, share and otherwise use information about you set out below:

• Name	• Telephone and email contact details	• Date of Birth
• Address	• Assessment information	• Details of previous/future schools
• Unique pupil number	• Behavioural information	• Language(s)
• Eligibility for free school meals	• Attendance information	• CCTV images

• Where you go to after you leave school	• Photographs	

We will also collect, hold, share and otherwise use some information about you which is called "special category personal data" and we will take extra care to make sure that this is kept safe:

• Racial or ethnic origin	• Religious beliefs	• Special educational needs and disability information
• Medical/health information	• Genetic and biometric data	• Information relating to keeping you safe
• Sexual life	• Sexual orientation	• Dietary requirements

Where do we get this information from?

We get this information from:

- you;
- your parents/carers;
- teachers and other staff; and
- people from other organisations, like doctors or the local authority, for example.

Why do we use this information?

We use this information for lots of reasons, including:

- to make sure that we give you a good education and to support you during your time at our school;
- to monitor and report on your progress;
- to make sure that we are able to address and support any educational, health or social needs you may have;
- to make sure everyone is treated fairly and equally;
- to keep you and everyone at the school safe and secure;
- to deal with any emergencies involving you;
- to celebrate your achievements;

- to provide reports and additional information to your parents/carers
- to assess the quality of our services;
- to comply with the law regarding data sharing.

Some of these things we have to do by law. Other things we do because we need to so that we can run the school. The UK General Data Protection Regulations (GDPR) provide a framework of Articles about the use of personal data. We have included a cross reference to the relevant Articles in the information below.

The use of your information for these purposes is lawful for the following reasons:

- We are under a legal obligation to collect the information or the information is necessary for us to meet legal requirements, such as our duty to safeguard pupils. (**Article 6, 1c UK GDPR**)
- It is necessary for us to hold and use your information for the purposes of providing schooling and so we can look after our pupils. This function is in the public interest because everybody needs to have an education. (**Article 6, 1e UK GDPR**)
- Sometimes we need permission to use your information. This includes taking pictures or videos of you to be used on our website or in the newspaper. Before we do these things we will ask you, or if necessary your parent/carer, for permission. (**Article 6, 1a UK GDPR**)
- If you give your consent, you may change your mind at any time and withdraw your consent by contacting DPO@deltatrust.org.uk.
- If we think that you will not understand what we are asking then we will ask your parent or carer instead. Usually, we will involve your parents even if you can make your own decision.

When we collect personal information on our forms, we will make it clear whether there is a legal requirement for you / your parents/carers to provide it, whether there is a legal requirement on the school / academy trust to collect it. If there is no legal requirement then we will explain why we are asking for it, how we plan to use it and provide an alternative if you chose not to provide consent.

Why do we use special category personal data?

We may need to use the information about you which is special (mentioned above) where there is a specific interest to do so, for example health and social care purposes (**Article 9, 2i UK GDPR**) or to provide you with equal opportunities and treatment (**Article 9, 2g UK GDPR**) We will also use this information where you have given us permission to do so (**Article 9, 2a UK GDPR**).There may also be circumstances where we need to use your information in relation to legal claims (**Article 9, 2f UK GDPR**) , or to protect your vital interests and where you are unable to provide your consent (**Article 9, 2c UK GDPR**).

How long will we hold information in relation to our pupils?

We will hold information relating to you only for as long as necessary. How long we need to keep to any information will depend on the type of information. Where you change school we will usually pass your information to your new school. If you would like more information about how long we keep information, please ask for a copy of our Personal Data Retention Policy. When we no longer need to retain information, we will destroy or delete it in a secure manner.

Who will we share pupil information with?

We will normally give information about you to your parents or your main carer. Where appropriate, we will listen to your views first. We will also take family circumstances into account, in particular where a Court has decided what information a parent is allowed to have.

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so.

We may share information about you with:

- other schools or educational institutions you may attend or require support from Local Authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes;

- the Department for Education and ESFA, as required by the law;

- contractors, to enable them to provide an effective service to the school, such as school meal providers or external tutors;

- non-LA professionals, medical professionals, educational psychologists, school nurse, school Counsellor or CAMHS (Child and Adolescent Mental Health Service);

- education and homework software systems. Depending on your school, this may include systems to help you practice timetables and spelling, to help with homework or revision in GCSE subjects or to show you reward points you have earned at school. These systems relate to our public task to provide you with an education. If you would prefer to do these activities without using the systems your school has put in place, please let your teacher know and we will arrange an alternative for you;

- our chosen independent careers services, Careers Inc. The information that is shared allows the careers advisor to provide informed and tailored guidance and advice to each pupil.

The information disclosed to these people / services may include sensitive personal information about you. Usually this means information about your health and any special educational needs or disabilities which you have. We do this because these people need the information so that they can support you.

A parent / carer can request that **only** their child's name, address and date of birth be passed to the local authority by informing the Principal. This right is transferred to the child once he / she reaches the age 16.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls, which meet the current government security policy framework.

The DfE may also share information about pupils that we give to them, with other people or organisations. This will only take place where the law, including the law about data protection allows it. If you would like more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

If you would like information about the organisations the department has shared pupil information with and why, please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received.

You can contact the DfE via : https://www.gov.uk/contact-dfe

Keeping this information safe

It is very important that only people who need to use your information can see it. The school keeps your information safe by:

- Encryption and password protection
- Network controlled permissions
- Secure disposal
- We do not normally transfer your information to a different country, which is outside the European Economic Area.

Your rights in relation to your information

You can ask to see the information we hold about you. If you wish to do this you should contact the Academy Office or you can email DPO@deltatrust.org.uk

You also have the right to:

- object to what we are doing with your information;
- have inaccurate or incomplete information about you amended;
- ask us to stop doing certain things with your information in some cases;

- ask that decisions about you are not made using automatic systems;
- claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights
- ask us to transfer your information to another organisation in a format that makes it easy for them to use.
- change your mind, if we have asked for your consent to use your personal data.

If you would like to do any of the above, you can speak to the Academy Office or you can email DPO@deltatrust.org.uk. We may not have to meet all of your requests and we will let you know where we are unable to do so.

Concerns

If you are concerned about how we are using your personal data then you can speak to the Academy Office or you can email DPO@deltatrust.org.uk, or if necessary you or your parent/ carer can contact an outside agency - the Information Commissioner's Office who could also help at https://ico.org.uk/concerns/

APPENDIX 7 – PRIVACY NOTICES: HOW WE USE SCHOOL WORKFORCE INFORMATION

This notice explains what personal data (information) we hold about you, how we collect it and how we use and may share information about you. We are required to give you this information under data protection law.

As an employer, the Trust collects and processes your personal data for employment and application for employment purposes. We will process your personal data in accordance with the UK General Data Protection Regulations and other relevant legislation, and not disclose your personal data to any other third party, unless allowed or required to do so under the relevant legislation.

Who are we?

Delta Academies Trust collects, uses and is responsible for certain personal information about you. When we do so we are regulated under the UK General Data Protection Regulation and we are responsible as 'controller' of that personal information for the purposes of those laws. Our Data Protection Officer can be contacted via DPO@deltatrust.org.uk.

The categories of school information that we collect and process include:

In the course of employing staff in our organisation we collect the following personal information when you provide it to us:

- Personal information (such as name, employee or teacher number, national insurance number)
- Characteristics information (such as gender, age, ethnic group)
- Contract information (such as start date, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Relevant medical information

This list is not exhaustive. If you have queries or would like further information about the categories of data we process, please contact DPO@deltatrust.org.uk.

Why we collect and use workforce information

We use workforce data to:

- enable individuals to be paid;
- support pension payments and calculations;

- enable sickness monitoring;
- enable leave payments (such as sick pay and maternity leave);
- develop a comprehensive picture of the workforce and how it is deployed;
- inform the development of recruitment and retention policies;
- inform financial audits of the organisation or individual academies;
- fulfil our duty of care towards our staff;
- inform national workforce policy monitoring and development

How long your personal data will be kept

We will hold information relating to you only for as long as necessary. How long we need to keep to any information will depend on the type of information. If you would like more information about how long we keep information, please ask for a copy of our Personal Data Retention Policy at your school or email DPO@deltatrust.org.uk. When we no longer need to retain information, we will destroy or delete it in a secure manner.

Reasons we can collect and use your personal information

We rely on having a legitimate reason as your employer to collect and use your personal information, and to comply with our statutory obligations, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

Under the UK General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:

Processing basis 1: Processing is necessary in order to meet our duties as an employer (**Article 6, 1 c UK GDPR** compliance with a legal obligation and **Article 9, 2b UK GDPR** carrying out obligations and exercising specific rights in relation to employment).

Processing basis 2: Processing necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract (**Article 6, 1b UK GDPR** re contract of employment or for the provision of a service to commercial client).

Processing basis 3: the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes (**Article 6, 1a UK GDPR and 9, 2a UK GDPR**). If you give your consent, you may change your mind at any time and withdraw your consent by contacting DPO@deltatrust.org.uk.

We are required to share information about our workforce members under section 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

Who we share your personal information with

- HM Revenue and Customs
- Pension Schemes
- Healthcare, social and welfare professionals and organisations
- The Disclosure and Barring Service
- Central Government Departments
- Educators and Examining bodies
- Professional Bodies
- Law enforcement agencies and bodies
- Courts and Tribunals
- Legal representatives
- Ombudsman and Regulatory bodies
- Service providers
- Trade Unions

With your explicit consent, we will share information with:

- Credit Reference Agencies;
- Mortgage Providers, Housing Associations and landlords.

To support TUPE arrangements the minimum necessary personal data and special categories of personal data will only be passed to the new employer.

We will share personal information with law enforcement or other authorities if required by applicable law, for example in relation to the prevention and detection of crime, counter terrorism, safeguarding, legal proceedings or to protect interests of you or another.

Collecting workforce information

We collect personal information via applications, new starter forms, contracts, change of personal details forms and by data collection forms as and when required which would be signed by the employee.

Workforce data is essential for the academy's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with UK GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this. You can withdraw your consent for the processing of your personal data at any time if that processing is on the sole basis of your consent (Processing basis 3).

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. If you would like a copy of our data retention schedule, please contact DPO@deltatrust.org.uk.

Who we share workforce information with:

We routinely share this information with the DfE.

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

Department for Education (DfE)

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by the DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the DfE: https://www.gov.uk/contact-dfe

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce;
- links to school funding and expenditure;
- supports 'longer term' research and monitoring of educational policy.

Your rights in relation to your information

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact DPO@deltatrust.org.uk.

You also have the right to:

- object to what we are doing with your information;
- have inaccurate or incomplete information about you amended;
- ask us to stop doing certain things with your information in some cases;
- ask that decisions about you are not made using automatic systems;
- claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights
- ask us to transfer your information to another organisation in a format that makes it easy for them to use.

- change your mind, if we have asked for your consent to use your personal data.

We may not have to meet all of your requests and we will let you know where we are unable to do so.

Concerns

If you have any concerns about how we are using your personal data then we ask that you contact our Data Protection Officer in the first instance, via DPO@deltatrust.org.uk. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Contact

If you would like to discuss this privacy notice, please contact: DPO@deltatrust.org.uk

APPENDIX 8 – PRIVACY NOTICES: PARENT / CARER PRIVACY NOTICE

Policy Statement

Information that we hold in relation to individuals is known as their "**personal data**".

During your child's time with us, we will gather and use information relating to you.

This will include data that we obtain from you directly and data about you that we obtain from other people and organisations.

We might also need to continue to hold your personal data for a period of time after your child has left the Academy. Anything that we do with an individual's personal data is known as "**processing**".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we process in relation to you?

We will collect, hold, share and otherwise use the following information about you:

- personal information (such as name, address, home and mobile numbers, personal email address, emergency contact details and relationship/ marital status);
- financial details (such as bank account or credit card details), and other financial details such as eligibility for free school meals or other financial assistance;
- CCTV footage and images obtained when you attend the Academy site; and
- your relationship to your child, including any Court orders that may be in place.

We may also use special categories of data such as ethnic group, sex or sexual orientation, religious or similar beliefs and information about health. These types of personal data are subject to additional requirements.

Where do we get your personal data from?

We will obtain an amount of your personal data from you, by way of information gathering exercises at appropriate times such as when your child joins the Academy and when you attend the Academy site and are captured by our CCTV system.

We may also obtain information about you from other sources. This might include information from the local authorities or other professionals or bodies, including a Court.

Why do we use your personal data?

Some of these things we have to do by law. Other things we do because we need to so that we can run the school. The UK General Data Protection Regulations (UK GDPR) provide a framework of Articles about the use of personal data. We have included a cross reference to the relevant Articles in the information below. We will process your personal data for the following reasons:

1. Where we are required by law (**Article 6, 1c UK GDPR**) , including:

    - To provide reports and other information required by law in relation to the performance of your child;
    - To raise or address any concerns about safeguarding;
    - To provide information to Government agencies, including the police;
    - To obtain relevant funding for the school; and
    - To provide or obtain additional services including advice and/or support for your family.

2. Where the law otherwise allows us to process the personal data as part of our functions as an Academy, or we are carrying out a task in the public interest (**Article 6, 1e UK GDPR**) , including:

    - To confirm your identity;
    - To communicate matters relating to the Academy or Trust to you;
    - To safeguard you, our pupils and other individuals;
    - To enable payments to be made by you to the Academy or Trust;
    - To ensure the safety of individuals on the Academy or Trust site; and
    - To aid in the prevention and detection of crime on the Academy or Trust site.

3. Where we otherwise have your consent (**Article 6, 1a UK GDPR**)

Whilst the majority of processing of personal data we hold about you will not require your consent, we will inform you if your consent is required and seek that consent before any processing takes place. If you give your consent, you may change your mind at any time and withdraw your consent by contacting DPO@deltatrust.org.uk.

Why do we use special category personal data?

We may process special category personal data in relation to you for the following reasons:

1. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy (**Article 9, 2g UK GDPR**).

2. Where the processing is necessary in order to ensure your health and safety on the Academy or Trust site, including making reasonable adjustments for any disabilities you may have (**Article 9, 2g UK GDPR**) .

3. Where we otherwise have your explicit written consent (**Article 9, 2a UK GDPR**).

There may also be circumstances where we need to use your information in relation to legal claims (Article 9, 2f UK GDPR), or to protect your vital interests or those of your child, and where it is not possible to seek your consent (**Article 9, 2c UK GDPR**).

Failure to provide this information

If you fail to provide information to us, we may be prevented from complying with our legal obligations.

How long will we hold your personal data for?

We will hold information relating to you only for as long as necessary. How long we need to keep to any information will depend on the type of information. This is laid out in our Data Retention Policy. If you would like a copy of this policy, please contact DPO@deltatrust.org.uk. When we no longer need to retain information, we will destroy or delete it in a secure manner.

Who will we share your personal data with?

We routinely share information about you with:

- Local authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes;

- The Department for Education and/or the Education and Skills Funding Agency, in compliance with legal obligations of the school to provide information about students and parents as part of statutory data collections; and

- Contractors, such as payment processing providers to enable payments to be made by you to the Academy or Trust.

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data.

Contact details for the Department can be found at https://www.gov.uk/contact-dfe.

Local authorities may share information that we are required to provide to them with other organisations. For further information about the local authority's data sharing process, please visit their website.

Your rights in relation to your personal data held by us

You have the right to request access to personal data that we hold about you, subject to a number of exceptions. To make a request for access to your personal data, you should contact:

Academy Office or DPO@deltatrust.org.uk

Our Data Protection Policy provides further details on making requests for access to your personal data. If you would like a copy of this policy, please contact DPO@deltatrust.org.uk.

You also have the right, in certain circumstances, to:

- object to what we are doing with your information;
- have inaccurate or incomplete information about you amended;
- ask us to stop doing certain things with your information in some cases;
- ask that decisions about you are not made using automatic systems;
- claim against the school in certain circumstances where you have suffered as a result of the school breaching your data protection rights
- ask us to transfer your information to another organisation in a format that makes it easy for them to use.
- change your mind, if we have asked for your consent to use your personal data.

If you want to exercise any of these rights then you should contact the Academy Office or DPO@deltatrust.org.uk. We may not have to meet all of your requests and we will let you know where we are unable to do so.

Concerns

If you have any concerns about how we are using your personal data then we ask that you contact our Data Protection Officer in the first instance, via DPO@deltatrust.org.uk. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/.

Contact

If you would like to discuss anything in this privacy notice, please contact:

DPO@deltatrust.org.uk

APPENDIX 9 – FREQUENTLY ASKED QUESTIONS

Q: What should I do if I receive a subject access request?

A: All subject access requests must be sent to the Data Protection Officer via DPO@deltatrust.org.uk. The Data Protection Officer will send the individual a Data Subject access request form.

Q: Can we charge someone who makes a subject access request?

A: We must respond to a subject access request and provide the information requested free of charge. However, in very limited circumstances, we may be able to charge a reasonable fee, taking into account the administrative costs of providing the information. Employees should contact the Data Protection Officer if they receive a subject access request.

Q: If someone asks us to delete all of the personal information we hold about them, do we have to comply with this request?

A: This may depend on what we require the personal data for. If, for example, the personal data is no longer necessary for the purposes for which it was collected or processed, or if the personal data has been unlawfully processed, then we must comply with the request. If an employee receives any such request, they should notify the Data Protection Officer. However, please note that we are obliged to keep pupil information in line with requirements set out in the Trust Personal Data Retention Policy. In addition, much of the employee data we hold will continue to be required even after someone no longer works for us.

Q: Can an individual get access to all data which mentions or refers to them when they make a subject access request?

A: No. If releasing the personal data would adversely affect the rights and freedoms of others (for example, if a document refers to a third party's personal data), then we can limit the information which we provide, for example, by redacting any references to third party personal data. If releasing personal data would, for example, disclose trade secrets, or affect intellectual property rights, we can limit the information which we provide to the individual.

If we process a large quantity of information about an individual, we are entitled to ask the individual, before delivering that information, to specify the information or processing activities to which their request relates.

Q: What should I do if I think I have lost some personal data or become aware someone else has lost some data (for example the loss of a laptop)?

A: Report this immediately to the Data Protection Officer using a Data Security Breach Incident Form (see Appendix 3).

Q: An individual has asked that we provide them with their personal data as they wish to provide this to another organisation. Are we obliged to do so?

A: In certain circumstances, yes. However, this will only apply to information that an individual has provided to us, and not information that has been obtained from other sources.

If we are obliged to comply with such a request, and the individual so requests, we must transmit such information directly to the other organisation, if this is technically feasible.

We must not provide any information which would adversely affect the rights and freedoms of others. For example, any information provided must not disclose the personal data of third parties.

Q: What should I do if the employee of a supplier calls over the telephone and asks for details of their personal data?

A: We should only disclose it if we can be sure of the identity of the caller. Personal data should only be provided to the Data Subject itself (and not to a third party) unless you have clear proof that the Data Subject allows the disclosure of data to such third party (such as a spouse or legal representative). If it is not possible to identify the caller using security questions, you should ask the caller to put their request in writing and pass the completed request to the Trust's Data Protection Officer.

Q: If an email is sent to the wrong person, do I need to do anything?

A: Yes. You should notify the Data Protection Officer immediately and complete the Security Breach Incident Form at Appendix 3 as comprehensively as possible.

Q: What should I do if I realise, or I am told that some of the personal data we hold is not accurate?

A: Inform the person who has authority to amend the data that it is inaccurate or make the amendment yourself, if applicable. However, if you know the data is correct you do not need to alter our record but you should put a note on the record that the Data Subject disputes this information is correct.

Q: What should I do if somebody complains about the way I am using their personal data?

A: You should take details of their complaint including contact details and tell them that we will respond as soon as possible. You should put the information in the Data Protection Complaint Form set out in Appendix 6 or ask the Data Subject to submit a form. You should then consider the purpose for which the personal data was collected and whether the way we are using the data is in accordance with that purpose.

Q: If a person with parental responsibility for a pupil / student asks for information about that pupil / student, can I provide it to them?

A: In summary, as the person with parental responsibility is, in effect, exercising that pupil's / student's right of subject access on that pupil's / student's behalf, then you must be satisfied that:

- the person making the subject access request does in fact have parental responsibility for that pupil / student; and either:
- the pupil / student is under 13 years of age or is 13 or over but is deemed not sufficiently mature and aware to understand the nature of a subject access request; or
- the pupil / student is aged 13 or over and is sufficiently mature and aware to understand the nature of a subject access request and
- the pupil / student has granted his/her authority to his/her personal data being disclosed to the person making the subject access request; or
- the pupil / student has made the subject access request himself / herself.

If the subject access request is not made by the pupil / student, including where the request is made by a person with parental responsibility for them, but that pupil / student is aged 13 or over and is sufficiently mature and aware and objects to any disclosure of his/her personal data, this objection should be respected and no disclosure of that personal data should be made.

Q: I can't breach the Data Protection Legislation just by talking about personal data, can I?

A: The Data Protection Legislation can be breached if you talk about another person's personal data which is held by the Trust, whether inadvertently or intentionally.

APPENDIX 10 – ROLES AND RESPONSIBILITIES

DPO	Responsible for: • Informing the Trust (as data controller) and member schools of their obligations in respect of data protection under the Data Protection Legislation and other relevant legislation. • Reviewing policies and practices within the Trust in relation to the protection of personal data. • Providing advice to the Trust on matters regarding compliance with Data Protection Legislation where appropriate or requested. • Keeping knowledge of law and practice in respect of data protection and information law up to date including identifying and attending appropriate training as agreed by management. • Assisting/overseeing any response to requests from Data Subjects relating to their rights in respect of their personal data in a timely manner and within the timeframes specified by law, including but not limited to Subject Access Requests. • Acting as the direct contact with the Information Commissioner's Office (ICO) as necessary, including but not limited to any direct enquiries from the ICO or reporting any reportable breaches. • Reporting directly to the Audit and Risk Committee of the Board of Trustees. • Having due regard of the risk associated with processing personal data and take into account the nature, scope, context and purposes of processing.
Principals	Responsible for: • Ensuring that Data Protection Legislation practice and information governance in schools meets the required standard. • Ensuring that information governance is integrated into all elements of school practice and is considered as part of new contract agreement or service design. • Ensuring all contracts are signed by the CFOO, as per the Trust Scheme of Delegation. • Ensuring that FOI requests, SARs or other live information governance issues are referred to the team around the DPO.

	• Supporting any investigation of reported breach or standards in school. • Ensuring that information security and governance policies are observed throughout the school.
Data Protection Lead in School	• Raise awareness of Data Protection in the Academy. • Raise awareness of the Trust's Data Protection and Retention Policies. • Report data breaches to the Trust DPO. • Maintain a log of Data Protection breaches. • Promote good practice in line with the Data Protection Policy. • Attend additional training and network meetings as required. • Notify the team around the DPO of any changes in school, which should be considered against information governance requirements including negotiation of new contracts, process changes and staffing.
AAB Members	• AABs are encouraged to include Data Protection Legislation within the finance, compliance and VFM scrutiny role. The link member to include information governance, as appropriate, in their termly report to the AAB.
All staff	• Support good information governance practice across the Trust, complying with data protection law and Trust policies at all times. • To ensure that any potential information breach is reported to the DPO and to support any investigation where required. • To undertake training at an appropriate level, seeking further guidance where required.

APPENDIX 11 – DATA PROTECTION IMPACT ASSESSMENT

Part 1– DPIA Triage Document

If personal data is being processed use the below form to work out if a full DPIA is needed. If you have a "yes" answer you need to conduct a full DPIA unless the processing is not "likely to result in a high risk". If this is the case, the you must justify and document the reasons for not carrying out the DPIA and include the view of the Data Protection Officer.

Where you complete the below form with a "No" in each section, then a DPIA may not be necessary but this completed questionnaire should be kept as evidence that a DPIA was considered.

	Processing Activity	Yes	No	Unsure (explain)
1.	Does the proposal involve any evaluation or scoring including profiling and predicting using information about a person?			
2.	Does the proposal involve any automated decision making which has a legal or similar legal effect e.g. whether to employ an individual?			
3.	Does the proposal involve any systematic monitoring: processing used to observe, monitor or control individuals, including data collected through networks e.g. employees' activities, including the monitoring of the employees' work station, internet activity; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation; includes internet tracking and profiling for behavioural advertisement?			
4.	Does the proposal involve any special category information or information of a highly personal nature e.g.			

	health/ethnicity/political beliefs/religion/sexual orientation/criminal offence/identity data or personal financial data?			
5.	Does the proposal involve data processed on a large scale? Large scale is not defined but should consider: A) The number of Data Subjects, either as a specific number or as a proportion of the relevant population. B) The volume of data and/or the range of different data items processed. C) The duration, or performance of the data processing activity. D) The geographical extent of the processing activity. Processing of patient/pupil data in the regular course of business by a hospital or school would be classed as "large scale" while processing of patient/pupil data by an individual physician/tutor would not.			
6.	Does the proposal involve any matching or combining of datasets? i.e. matching two or more data processing operations performed for different purposes in a way that would exceed the reasonable expectations of an individual.			
7.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, and cases where an imbalance in the relationship between the position of			

	the individual and the controller can be identified.			
8.	Does the proposal involve any innovative use or applying new technological or organisational solutions e.g. combining use of finger print and face recognition for improved physical access control?			
9.	Does the proposal involve any processing which in itself 'prevents Data Subjects from exercising a right or using a service or contract' e.g. determining eligibility based on an individual's circumstances?			

Part 2 – Data Protection Impact Assessment

[Insert Organisation Name]

[Insert Project Name]

Data Protection Impact Assessment

Version	
Purpose of Document	Identifies any impact on privacy where a new service or system is introduced or where there is a change in law
Ratified By	[*insert name of relevant committee or person e.g. Head of Compliance/ Compliance Committee*]
Date Agreed	
Review Date	[*DPIA's should be reviewed periodically to ensure they are still relevant*.]
Name of Author and contact details	

1. **Executive Summary**

1.1. [*Complete with overall conclusions on privacy issues under the project and how these may be resolved*].

2. **Introduction**

2.1. [The Company] would like to deliver a project to [insert outline description of the project] (the "**Project**").

2.2. The UK General Data Protection Regulation and the Data Protection Act 2018 (together the Data Protection Laws) set out a framework to safeguard personal data. The Project [insert general description of how personal data is processed under the Project].

2.3. This Data Protection Impact Assessment (DPIA) should:

2.3.1. [describe purposes and objectives of the Project];

2.3.2. [assess the potential implications for privacy];

2.3.3. [explain what the organisation will do to protect privacy]; and

2.3.4. [meet the ICO guidelines for projects such as this and meet certain legal requirements in respect of Data Protection Laws]

2.4. This DPIA has been carried out by [insert name] [with the assistance of [insert names of those who help including any processors]. If you want to discuss the conclusions of this DPIA please contact [ ] on [insert email address and phone number.]

3. Purpose of the Data Protection Impact Assessment

3.1. The purpose of the DPIA is to assist organisations to assess the possible impact a proposed project may have on personal data held by the organisation; to assess whether any action can be taken to minimise any increased data risk caused by the Project. They encourage a data protection by design and default approach and ensure compliance with Data Protection Laws.

3.2. Carrying out a DPIA is a legal requirement under Data Protection Laws where the processing is likely to result in a high risk to the rights and freedoms of Data Subjects (particularly if it involves the use of new technologies). Even in cases where it is not clear that a DPIA is required, we should consider carrying one out nonetheless, as conducting a DPIA is not only a useful aid to assist us in complying with Data Protection Laws, it also demonstrates our commitment to privacy and will help develop projects with a privacy by design approach. This should:

3.2.1. identify and manage risk;

3.2.2. avoid unnecessary costs by avoiding the need to retro-fit functionality into a system to ensure legal compliance;

3.2.3. avoid inadequate solutions;

3.2.4. inform the organisation's communications strategy in respect of the Project both internally and externally; and

3.2.5. meet and exceed the organisation's legal expectations.

3.3. In carrying out this DPIA we have considered the following guidance:

3.3.1. The ICO's guidance on DPIAs: "Conducting Privacy Impact Assessments Code of Practice";

3.3.2. The Article 29 Data Protection Working Party guidelines on DPIAs and whether processing is likely to result in a high risk under Data Protection Laws; and

3.3.3. [other ICO guidance]

3.4. This Project has been identified as one requiring a DPIA because [insert summary as to why a DPIA is required for this project e.g. it involves processing of high risk data as set out in Data Protection Laws or otherwise it affects a large number of people, uses intrusive technologies, uses existing data for a new purpose or involves processing of sensitive or criminal data]

3.5. This DPIA should be stored together with the Project files to demonstrate the procedures put in place to safeguard personal data.

3.6. The DPIA will be kept under review and revised as the detail for each phase of the Project is developed. We welcome feedback on this DPIA.

3.7. Where this DPIA indicates that despite mitigating measures identified through the DPIA that the processing remains a high risk, this DPIA shall be notified to the ICO and the organisation shall enter discussions on the Project and this DPIA.

4. **Project Description**

4.1. The Project [*provide an outline description of the Project*]. This will involve changes to [*insert description of existing processes, systems or technologies which must be changed]*.

4.2. The Project involves the processing of [*insert description of personal data to be processed. This should include collection, use and deletion of information. It may be useful to describe data flows.*]

4.3. [*describe who the information is about. This should state if the individuals are employees, customers, suppliers or other categories. Describe any consultation process there may be with individuals.]*

4.4. [*describe who will process the information e.g. internal staff or external contractor*]

4.5. [*describe where the personal data will be held. If personal data is to be held by a third party describe the process of how the personal data will be created and processed by the third party, whether a contract exists and the outline data protection provisions within that contract*]

4.6. [*describe who has access to the personal data (both internally and by any third party service providers) and how access rights will be managed*]

4.7. [*describe how the personal data will be checked for accuracy – consider this in the context of the start of the Project and for ongoing processing*]

4.8. [*describe if the Project will process sensitive or high risk personal data. Sensitive personal data is personal data relating to racial or ethnic origin, political or religious beliefs or opinions, health, sexual life, offences and court proceedings. High risk personal data is personal data that can lead to identity theft or fraud such as National Insurance Number, Passport Number, Driving Licence details or financial information*.]

4.9. [*describe the security arrangements. This should include technical and organisational security. E.g. will files be password protected and encrypted? Will the system be security tested before go-live? Is there a physical security aspect to the Project? How will you ensure that individuals involved in the Project who handle personal data are properly trained? Where third parties are being used, this should include a description of the measures taken by the third party and any due diligence and continuing monitoring undertaken by the organisation*]

4.10. [*Will personal data be transferred or stored (for example on servers) outside the UK? Describe the measures which have been taken to ensure there are adequate safeguards to ensure compliance with the UK GDPR in such processing. Consider where data will be stored by any third party service provider*]

5. **Compliance**

5.1. Processing of personal data under the Project is permitted by [*insert the Article 6 processing condition(s) which is being relied on to process the personal data. If special category data is also being processed you should also state the Article 9 processing condition which is being relied on. Where criminal data is being processed you must comply with Article 10. If consent is being used, identify where that consent was obtained and the surrounding circumstances. If a legitimate interest is being relied on you should state the legitimate interest and carry out and document a legitimate interest assessment*.]

5.2. [*Fair processing? Insert a description of how the organisation believes that it is undertaking fair processing. Are there issues of confidentiality? Is there a fair processing notice?*]

5.3. [*Describe if compliance with any other laws is affected by this Project.*]

5.4. [*Insert description of the risk review process – describe how the outcomes of the DPIA are integrated into the Project plan*]

6. **What privacy issues arise under the Project?**

6.1. The following privacy issues were identified within the Project:

6.1.1. Risk 1 e.g. proposal to host personal data at hosted facility in US

6.1.2. Risk 2 e.g. no fair processing notice issued to inform Data Subjects how personal data is to be processed.

6.1.3. Risk 3 e.g. the Project involves the processing of sensitive personal data

6.1.4. Risk 4 e.g. the use of personal data gathered by the Project for other purposes

6.1.5. Risk 5 e.g. period of time the personal data should be held

6.1.6. Risk 6 e.g. access rights held by a large number of individuals at the service provider

6.2. Risk 1

6.2.1. Describe the issue

6.2.2. Describe how this is a risk to individuals/what impact this will have on individual's privacy

6.2.3. Describe how the risk is addressed in the Project (i.e. the solution; does it treat, remove, tolerate or transfer the risk; what controls are put in place?)

6.2.4. Evaluate the response to the risk

6.3. Risk 2 [repeat above points]

6.4. Risk 3 [repeat above points]

6.5. Risk 4 [repeat above points]

6.6. Risk 5 [repeat above points]

7. **Business Case for Processing of Data under the Project**

7.1. The fundamental purpose of the Project is to [*insert description of purpose of Project*]. In order to make this assessment we need to [*insert the business case for the Project e.g. greater accountability, need to embrace new technologies, greater efficiencies*].

8. **Alternatives to Processing Personal Data**

8.1. Due to the nature of the personal data gathered through the Project it is possible that certain generic lessons could be learned from the data. [insert statement re possible use of anonymised data in the Project].

APPENDIX 12 – APPROPRIATE POLICY DOCUMENT

Appropriate Policy Document

1. About this policy

1.1 This is the appropriate policy document for Delta Academies Trust ("the "**Controller**") setting out how we will protect special categories of personal data and criminal offence data.

1.2 Many of the conditions for processing special category and criminal offence data under the Data Protection Laws require us to have an appropriate policy document in place, setting out and explaining our procedures for securing compliance with the six data protection principles of the UK GDPR and policies regarding the retention and erasure of such personal data. This document explains our processing and satisfies the requirements of the Data Protection Laws.

1.3 This policy supports Delta Academies Trust's Data Protection Policy and adopts its definitions.

2. What is special category data?

2.1 Special category data is defined at Article 9 of the UK GDPR being personal data about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying someone
- Data concerning health
- Data concerning someone's sex life or sexual orientation

3. What is criminal offence data?

3.1 Article 10 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, Section 11(2) of the Data Protection Act 2018 (DPA 2018) specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an

offence committed or alleged to have been committed, including sentencing. We refer to this as 'criminal offence data'.

4. Why we process special categories of personal data and criminal offence data:

4.1 We process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the UK GDPR and Schedule 1 of the DPA 2018.

5. Compliance with the personal data protection principles

5.1 The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

5.2 We comply with the principles relating to processing of personal data set out in the UK GDPR which require personal data to be:

- processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency) (see Section 6);
- collected only for specified, explicit and legitimate purposes (Purpose Limitation – see Section 7);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation – see Section 8;
- accurate and where necessary kept up to date (Accuracy – see Section 9;
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation – see Section**Error! Reference source not found.**); and
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality – see Section 11.

5.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability – see Section 12.)

6. Lawful, fair and transparent processing

6.1 We must only process personal data in a lawful, fair and transparent manner.

6.2 The UK GDPR restricts our actions regarding personal data to specified lawful purposes. We can process special categories of personal data and criminal offence data only if we have a legal ground for processing and one of the specific processing conditions relating to special categories of personal data or criminal offence data applies. We identify and document the legal ground and specific processing condition relied on for each processing activity in our privacy policy.

6.3 When we collect special categories of personal data and criminal offence data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we provide Data Subjects with our privacy policy setting out all the information required by the UK GDPR. We will provide this information in a way which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

6.4 We process special categories of personal data and criminal offence data in accordance with the following processing conditions:

- **Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law** on the ICO or the Data Subject in connection with employment, social security or social protection:

Examples of our processing here are staff sickness absences and assessments of the working capacity of the employee and processing employee data to make reasonable adjustments to the workplace, verifying that candidates are suitable for employment or continued employment political activity declarations,

- **Article 9(2)(g) – reasons of substantial public interest**

[[IN ORDER TO PROCESS DATA ON THE BASIS OF SUBSTANTIAL PUBLIC INTEREST YOU NEED TO HAVE A SUITABLE SUBSTANTIAL PUBLIC INTEREST CONDITION AS SET OUT IN PART 2 OF SCHEDULE 1 OF THE DPA 2018.]

- **Article 9(2)(a) explicit consent**

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our customers who require a reasonable adjustment to access our services.

- **Article 9(2)(c) processing necessary to protect vital interests**

An example of our processing would be using health information about a member of staff in a medical emergency.

We process criminal offence data under Article 10 of the UK GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

7. Purpose limitation

7.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

7.2 We will only collect personal data for specified purposes and will inform Data Subjects what those purposes are in our privacy notice. We will not use personal data for new, different or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

8. Data minimisation

8.1 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

8.2 We will only collect or disclose the minimum personal data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the personal data collected is adequate and relevant for the intended purposes.

9. Accuracy

9.1 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

9.2 We will ensure that the personal data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

10. Storage limitation

10.1 We only keep special category or criminal offence personal data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

10.2 We maintain a Data Retention Policy and related procedures to ensure personal data is deleted after a reasonable time has elapsed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

10.3 We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

11. Security, integrity, confidentiality

11.1 Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

11.2 We will implement and maintain reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of or damage to personal data. We will process electronic data within our secure networks and systems. Hard copy data is processed in accordance with our security policies. We operate appropriate access controls in all our systems.

12. Accountability principle

12.1 We are responsible for, and able to demonstrate compliance with these principles. The Data Protection Officer is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the Data Protection Officer.

We will:

- Ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request.
- Carry out a DPIA for any high-risk personal data processing to understand how processing may affect Data Subjects and consult the Information Commissioner if appropriate.
- Ensure that a Data Protection Officer is appointed to provide independent advice and monitoring of personal data handling, and that the Data Protection Officer has access to report to the highest management level.
- Have internal processes to ensure that personal data is only collected, used or handled in a way that is compliant with data protection law.
- Have policies on retention and erasure of personal data.

12.2 We take the security of special categories of personal data and criminal offence data very seriously. We have administrative, physical and technical safeguards in place to protect personal data against unlawful or unauthorised processing, or accidental loss or damage. We will ensure, where special categories of personal data or criminal offence data are processed that:

- The processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the different categories of data in accordance with our Personal Data Retention Policy.

- Where we no longer require special categories of personal data or criminal offence data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

- Where records are destroyed we will ensure that they are safely and permanently disposed of.

12.3 Data Subjects receive a copy of our privacy notice setting out how their personal data will be handled when we first obtain their personal data, and this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. We also make the privacy policy notice available on our website.

13. Additional special category processing

13.1 We also process special category and criminal offence data in other instances where it is not a requirement to keep an appropriate policy document. Where we do so we will comply with our legal obligations in respect pf the processing of those data. Our privacy policy [insert] contains clear, transparent and unambiguous information setting out the lawful bases for processing.

14. Review

14.1 This policy on processing special categories of personal data and criminal offence data is reviewed triennially.

14.2 The policy will be retained where we process special categories of personal data and criminal offence data and for a period of at least six months after we stop carrying out such processing.

14.3 A copy of this policy will be provided to the Information Commissioner on request and free of charge.

Dated:

Review date:

Next review:

For further information about our compliance with data protection law, please contact our Data Protection Officer at Delta Academies Trust, Education House, Spawd Bone Lane, Knottingley, WF11 0EP.

APPENDIX 13 – LEGITIMATE INTERESTS ASSESSMENT

LIA template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

1. **Purpose test**

1.1 Is a legitimate interest behind the processing?

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (e.g. profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

2. **Necessity test**

- Is the processing necessary for the purpose you have identified?
- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

3. **Balancing test**

3.1. Consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

3.2. Consider the ICO's DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

3.3. Nature of the personal data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

3.4. Reasonable expectations

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

3.5. Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

3.6. Can you offer individuals an opt-out?

Yes / No

4. **Making the decision**

This is where you use your answers to paragraphs 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

4.1. Can you rely on legitimate interests for this processing?

Yes / No

4.2. Do you have any comments to justify your answer? (optional)

LIA completed by:

Date:

5. **What's next?**

5.1. Keep a record of this LIA, and keep it under review.

5.2. Do a DPIA if necessary.

5.3. Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.