Data Protection Policy and Procedures

November 2019

CONTENTS

DOCUMENT CONTROL

Who is this policy for?

This policy applies to employees (including consultants, temporary and agency staff), Directors, 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, directors, pupils / students, people with parental responsibility for pupils / students and suppliers.

This Policy Statement

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

- the GDPR,
- our responsibility in respect of data protection practice,
- our rights and obligations
- why it is so important.

It applies to all actions we take which involve the processing of and working with personal data.

This policy statement and the supporting policy have been approved by the Audit and Risk Committee of the Trust's Board of Directors.

This Policy is maintained by the Data Protection Officer, who shall 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 If you are aware that this policy is incorrect or out of date, please inform the Data Protection Officer immediately.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 November 2020.

Revision History

REVISION	DATE	DESCRIPTION	AUTHOR
1	Nov 2018	Policy issued.	Emma Mayor
2	Nov 2019	Revised policy published after changes approved.	Emma Mayor

1. SUMMARY OVERVIEW

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.

1.2 The use of personal data is governed by the General Data Protection Regulation (the "GDPR") and the Data Protection Act, 2018.

1.3 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.

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

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

1.6 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

2.1 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

2.2 The GDPR regulate the processing of personal data. Personal data is data about a living individual, who can be identified from the data or from the data and other information which is available to us. Data bout businesses or organisations is not covered by the GDPR but data about their directors, partners, employees, customers and suppliers is.

2.3 We will process personal data in accordance with the GDPR. Processing includes obtaining, recording, holding, reading, using or destroying personal data.

2.4 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 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.

2.5 We will process personal data in accordance with the GDPR and good data protection practice.

2.6 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. We will make sure our fair processing notices are kept up to date and reflect the processing activities we undertake. Please see the appendices to this policy for Trust Fair processing notices (Privacy Notices)

2.7 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.

2.8 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).

2.9 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.

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

2.11 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.

2.12 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.

2.13 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 GDPR.

2.14 We 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.

2.15 The Data Protection Officer will report to the Board of Directors via the Audit and Risk Committee of the Trust.

HOW SHOULD PERSONAL DATA BE USED?

2.16 The GDPR outlines six core principals, which broadly set out the way in which personal data should be used. Personal data must be:

- Processed fairly, lawfully and in a transparent manner;
- Collected for specific, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of Data Subjects for no longer than is necessary for the personal data to be processed; and
- processed securely and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2.17 You should be Aware that the GDPR has a range of criminal offences, including personal liability, when you unlawfully obtain or sell personal Data. In addition, we can be fined for breaches of the GDPR.

2.18 Our compliance with our data protection policy and procedures will ensure compliance with our 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 fair processing notices.

2.19 Where we process personal data which is particularly sensitive, such as information about a person's health, religion or sex life or is 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.

2.20 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 GDPR.

KEEPING DATA SECURE

2.21 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.

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

2.23 We will work together with our IT team to ensure that where Trust employees Members and Directors (or, if applicable, volunteers) need to take laptops, tablets, memory sticks, smart phones or mobile phones 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 E-safety Policy for further information.

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

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

DATA RETENTION AND DESTRUCTION

2.26 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.

2.27 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.

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

STUDENT DATA

2.29 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 GDPR.

STAFF DATA

2.30 In the course of our recruitment and employment of staff, we will collect and process various data about them, including sensitive personal data. This information will be retained for the duration of their employment by us.

2.31 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, matters relating to retirement benefits and to allow us to fulfil contractual and statutory obligations.

2.32 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.

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

REQUESTS FOR DATA

2.34 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.

2.35 Requests should be made in writing 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.

2.36 When we receive requests for data, we are required to answer the request within a calendar month.

2.37 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.

2.38 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.

2.39 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.

2.40 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, Directors, contractors, AAB members or volunteers receive such a request, it must be promptly referred to the Data Protection Officer.

OTHER RIGHTS

2.41 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 data subject may request that the processing of their personal data be restricted.

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

DATA BREACH

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

2.43 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 out of the data breach.

2.44 A Data Security Breach Notification form is included in Appendix 3 to this policy.

2.45 A data breach log will be maintained by the Data Protection Officer who shall 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.

2.46 The data breach log shall be made available to the ICO or relevant supervisory authority if requested.

SHARING DATA WITH OTHER PEOPLE/ORGANISTIONS

2.47 We will not send personal data to a third party or another organisation, unless the data subject has given us their authority to do so, or we are otherwise permitted by law.

2.48 We will take care to consider whether the data subject has given authority to their data being passed to another organisation before we transmit the data.

2.49 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.

2.50 We will carry out due diligence, put in place contracts and/or data sharing

2.51 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/raising a Purchase Order with a supplier where you need to share data.

TRANSFERRING DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

2.52 We do not intend to transfer personal data outside the EEA.

2.53 Where it is necessary to do so, we will ensure any such transfer is carried out in accordance with the requirements of the GDPR in order to ensure that the level of protection to data subjects guaranteed by the GDPR is not undermined by any such transfer.

2.54 In the event that the United Kingdom leaves the European single market, we shall ensure that any transfer of personal data overseas is transferred in accordance with all applicable data protection legislation in place at the time of such transfer.

TRAINING

2.55 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.

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

CHANGES TO THIS POLICY

2.57 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.

2.58 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.

2.59 In the event that the United Kingdom leaves the European single market, we will ensure that we comply with any new data protection legislation that is enacted as a result.

3. LEGAL OBLIGATIONS ON PROCESSING

3.1 If you process personal data you must do so in accordance with the six Data Protection Principles. These state that personal data must be:

- processed fairly and lawfully and in a transparent manner (lawfulness, fairness and transparency);
- obtained for specified, explicit and lawful purposes and processed compatibly with those purposes (purpose limitation);
- adequate, relevant and not excessive for the purposes for which it is processed (data minimisation);
- accurate and up to date and every reasonable step must be taken to erase or rectify inaccurate data without delay (accuracy);
- kept no longer than necessary; and
- processed subject to appropriate security measures (integrity and confidentiality).

4. NOTIFICATION

4.1 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.

4.2 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.

4.3 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.

4.4 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

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

- a processing record;
- a data breach log
- a data breach policy;
- fair processing notices; and
- data protection impact assessments, as necessary, for certain projects.

PROCESSING RECORD

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

- the name and contact details of the data controller (and, where applicable, the joint controller, the data 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 to a third country or international organisation (where applicable), including the identity of the third controller 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.

4.7 If you are aware that the processing record is incorrect or out of date, please inform the Data Protection Officer immediately.

4.8 The processing record must be available to the ICO or relevant supervisory authority, if requested.

5. DATA PROTECTION BEST PRACTICE

5.1 We must process personal data in accordance with the GDPR. 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 GDPR;
- assuming overall responsibility for compliance with the GDPR;
- selecting someone to be responsible for ensuring compliance with the GDPR and making this person known to staff. This person is the Data Protection Officer;
- maintaining a record of how personal data is kept and processed and notifying the ICO in accordance with the GDPR; and
- maintaining other documentation including a data breach log.

5.2 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.

6. PROCESSING PERSONAL DATA

6.1 All personal data should be processed in accordance with the GDPR, the DPA and this policy.

6.2 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.

6.3 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 student or a person with parental responsibility for that 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.

6.4 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/Facebook/Twitter 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;
- office relocation activities involving the movement of personal data records; and
- disposal of confidential waste containing personal data.

6.5 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 GDPR

6.6 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 GDPR. All records should be clear and fair.

6.7 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 GDPR. 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.

6.8 You should only process data if one of the processing conditions set out in the 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; or
- there is another legitimate reason to process the personal data.

6.9 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.

6.10 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 or for medical purposes or in relation to a criminal investigation, you should make sure you obtain the explicit consent of an individual before processing sensitive data relating to them;
- If explicit consent has not or cannot be obtained (for example, you cannot use consent as a reason to process employee data), you must ensure that before any special categories of personal data are processed, one of the other special categories of personal data processing conditions set out in the GDPR apply. If you are unsure, please contact the Data Protection Officer;
- store all special categories of personal data with adequate 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 GDPR. 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.

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

DATA PROTECTION IMPACT ASSESSMENTS

6.12 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. Please contact the DPO at dpo@deltatrust.org.uk for more information.

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

- if we process, on a large scale, sensitive personal 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).

6.14 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 relations 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; and
- 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 GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

6.15 We will conduct impact assessments on the processing operations that the ICO publicly list as requiring impact assessments.

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

6.17 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.

6.18 If a processor is involved in the processing activity we should ask for their assistance in completing the DPIA. They are under a legal obligation to help us in this regard.

6.19 Please contact the DPO via dpo@deltatrust.org.uk for further information on DPIAs.

USING DATA PROCESSORS

6.20 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 pensions administration), we must ensure that they provide sufficient guarantees that they do, and will continue to, implement appropriate technical and organisational measures to ensure compliance with the GDPR and protect the personal data of Data Subjects.

6.21 We must 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.

6.22 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.

CONSENT

6.23 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.

6.24 For consent to be informed, a Data Subject should be aware of our identity as data controller; and the purpose(s) of the processing for which the personal data are intended.

6.25 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.

6.26 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.

6.27 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.

6.28 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.

6.29 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.

6.30 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 their employment with the Trust.

6.31 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

6.32 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.

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

6.34 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.

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

6.36 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.

6.37 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 authority over that child, unless it is evident that it would be against the best interests of the child to seek such parental consent.

6.38 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.

6.39 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 data, subject to completion of the competency assessment outlined above.

6.40 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.

6.41 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.

7. INFORMATION, INSTRUCTION AND SUPERVISION

7.1 A copy of this policy will be kept on the Trust VLE.

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

7.3 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.

7.4 Temporary staff 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 and new staff must not be allowed to carry out activities involving the processing of personal data until such training has been undertaken.

7.5 If you feel that you need additional training for a particular task or a refresher you should contact the Data Protection Officer who will arrange for additional training to be provided.

7.6 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 GDPR or other laws, you should check this with the Data Protection Officer.

8. COMPETENCY FOR TASKS AND TRAINING

8.1 We recognise that our employees are a key factor in supporting our effective and efficient operation and helping us to comply with data protection laws and good practice. We are committed to ensuring you receive training and development to help fulfil our legal and good practice obligations regarding the processing of personal data.

8.2 In the first instance, you 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.

8.3 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.

8.4 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. 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.

8.5 Annual refresher training will be provided.

8.6 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.

9. MONITORING THE USE OF PERSONAL DATA

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 Where we engage in a new way of processing personal data, we shall review that new method and ensure that any personal data so processed in accordance with the law and good practice.

10. PROVISION OF FAIR PROCESSING NOTICES

10.1 We must provide fair processing information to Data Subjects relating to the processing of their personal data.

10.2 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 EEA, 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 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; and
- 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.

10.3 Standard notices have been prepared and are included in the Appendices to this document.

10.4 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.

11. HANDLING AND STORING PERSONAL DATA AND DATA SECURITY

11.1 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;
- "Integrity" 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

11.2 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.

11.3 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.

11.4 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.

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

11.6 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

11.7 Manual data refers to paper and other non-digital personal data, records (such as copies of photographs or plans), which are recorded as part of a relevant filing system or with the intention that it should form part of such a system.

11.8 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 and a record should be kept of all such reviews.

11.9 Any documents containing personal data or sensitive personal data should not be left on a desk on view when the desk is unattended. For example, do not

leave HR records, CV's, pupil education records, parent/guardian data on desks when you leave your desk, even if it is just for a short time.

11.10 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 E-Safety Policy.

TECHNICAL SECURITY MEASURES

11.11 We will ensure that all computers have protection against malicious software/viruses and that software is not installed and information is not downloaded without first being checked for viruses and other malware. We will keep up to date with patches, fixes and new releases to ensure that our systems are protected against known security issues.

11.12 You should always store personal data electronically on our central computer system or on encrypted corporate devices and not on local drives or at home.

11.13 All computers and systems containing personal data should be password protected and all passwords should be kept secure at all times. Your passwords should include a mixture of letters and numbers and not be easy to guess or use common combinations - such as "1234". You must not use consecutive versions of the same password such as "Password 1", "Password 2". We will notify you when we require you to change your password. If you are concerned that someone may know your password, you must change your password immediately.

11.14 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 pass code 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.

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

11.16 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.

11.17 You should ensure that individual monitors are positioned so they do not show confidential information to passersby or people sitting in adjacent seats in public places. This is particularly important if your PC displays employee, pupil / student data or sensitive data. PCs must be locked or logged off when left unattended.

11.18 Where you use a memory stick to store information, you must use an encrypted memory stick provided by the IT department. You must not use unencrypted memory sticks to store personal data.

11.19 Please see the Trust E-Safety Policy for more details.

ORGANISATIONAL SECURITY MEASURES

MANUAL RECORDS

11.20 You should keep manual 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

11.21 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.

11.22 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.

BUILDING ACCESS

11.23 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

11.24 You must store personal data in a manner which enables it to be processed in accordance with the GDPR and DPA. 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

11.25 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.

11.26 The sale or destruction of all IT equipment including PCs, laptops, smart phones and other mobile devices 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.

11.27 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.

11.28 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.

11.29 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

11.30 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.

11.31 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.

12. PERSONAL DATA BREACH, NOTIFICATION AND REPORTING

INTRODUCTION

12.1 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.

12.2 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.

WHAT IS A PERSONAL DATA BREACH?

12.3 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.

12.4 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;
- the loss of a folder of papers or an electronic device such as a memory stick containing personal data in a public place; and
- 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?

12.5 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?

12.6 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 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.

12.7 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.

12.8 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.

12.9 We are required to notify the ICO or relevant supervisory authority, 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.

12.10 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.

12.11 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.

12.12 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/Representative (or other contact point where more information on the Personal Data Breach can be obtained);
- 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.

12.13 The ICO or other relevant supervisory authority is entitled to request a copy of our data breach log to verify our compliance with the GDPR. 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.

REVIEWING THE RESPONSE

12.14 Once the Personal Data Breach has been dealt with, we will appoint a team of individuals to 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.
- If applicable, the results of any review should be communicated to members of staff.

13. RIGHTS OF A DATA SUBJECT

13.1 We must put in place processes to enable Data Subject to exercise their legal rights.

13.2 A Data Subject has the following rights under the 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 data 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.

13.3 We must provide information requested by a Data Subject under the 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.

13.4 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, if a person with parental responsibility for that pupil or student, requests that pupil's / students educational record, such request will be made subject to the GDPR and not those regulations.

13.5 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

13.6 The Trust Subject Access Request form is attached as Appendix 2 to this policy.

14. THIRD PARTY REQUESTS FOR DATA

14.1 The GDPR 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.

14.2 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.

14.3 In such cases, an exemption included in the GDPR and DPA 2018 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.

14.4 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.

14.5 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.

14.6 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.

- 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)).

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

15. USE OF CCTV

15.1 CCTV systems process personal data. CCTV processing is intrusive by its nature and where public areas are monitored, specific concerns may be raised under the GDPR. 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 CCTV systems we operate. The record will contain:

- what cameras are kept and where;
- the purpose for the CCTV system. This should include an assessment of the process and the reasons for installation of the scheme; and
- confirmation that the CCTV system has been notified to the ICO.

15.3 CCTV equipment should be sited so that it only records that information which is necessary for the purpose of the scheme (i.e. it should not capture images of people not visiting the 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. Where the CCTV system records public areas and an outside contractor is used, the Trust shall carry out due diligence to ensure the contractor has appropriate licensing in place (if needed).

15.4 CCTV equipment 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. CCTV images contain personal data and should only be processed by the Trust in accordance with the GDPR. CCTV 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 ICT Team.

15.5 All CCTV 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 CCTV should have signs displayed indicating that individuals are entering a CCTV 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 CCTV 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.

15.10 CCTV images 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 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, CCTV 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 on the Every system.

15.14 If we are considering using an existing CCTV system for a new purpose, 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 General Data Protection Regulations; this means that it must be obtained, used and stored in accordance with GDPR.

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 General Data Protection Regulation.

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:

a) recording students' biometric data, for example, taking measurements from a fingerprint via a fingerprint scanner;

b) storing students' biometric information on a database system; or

c) 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/carer 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:

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

b) A parent or student has not consented in writing to the processing; or

c) A parent 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 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"). Whilst travelling you must either use a work laptop or device. 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 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 section 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 E-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 alone are responsible for all costs associated with the Device and 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 GDPR.

Term	Definition
"Data"	is information which is stored electronically, on a computer, or in certain paper-based filing systems. The GDPR 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 GDPR.
"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 data 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.

Term	Definition
"Data controllers"	are the people who, or organisations which, determine the purposes for which, and the manner in which, personal data is processed. They have a responsibility to establish practices and policies in line with the GDPR.
"Data processors"	include any person who processes personal data on behalf of a data controller. Employees of data 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 data using the same safeguards we operate with in respect of special category data.

19. APPENDIX 2 – SUBJECT ACCESS REQUEST FORM

1. Are you employed by the Trust? Yes No

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

_____

_

3. Please provide the details of the person requesting the information:

Full Name: _____

Address: _____

Telephone Number: _____

Email: _____

4. Are you the Data Subject? Yes No

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

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

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

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

6. 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: _____

7. If you are not the Data Subject, please provide:

7.1 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;

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

7.2.1 if the pupil / student is aged 13 or over and we deem that that pupil / student is able to understand the nature of, and make a subject access request himself / herself, proof that the pupil / student has authorised you to request data on their behalf (see 7.1); or

7.2.2 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 himself/herself), please provide:

7.2.2.1 evidence of your identity; and

7.2.2.2 if requested, evidence that you have parental responsibility for that pupil / student; and

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

Scope of Request

8. 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

9. 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 him or her.

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 pursuant 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. The individual should 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 EEA);
- 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. If a Data Subject makes a subject access request via electronic means, then unless they request otherwise, we shall provide any information to them in a commonly used electronic form (e.g. via secure e-mail).

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 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 GDPR.

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:

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).

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, then in addition to the exemptions contained within the GDPR, *The Data Protection (Subject Access Modification) (Education) Order 2000* (the **"Order"**) provides that certain information does 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 GDPR, the Order or any other statutory provisions, then you must contact the Data Protection Officer.

20. 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): _____

Data Processor

1. If a data processor or sub-processor was involved, was the data protection provisions within the contract entered into between the Trust and the data 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 directors)
- 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 GDPR they have a legal obligation to assist.

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

8. Under the 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 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 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.

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 subject; and
- the number of affected individuals.

15. Part of the classification of the risk is also dependent on our own characteristics as a data 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).

21. 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 E-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:_____

22. 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?

   Yes No

4. If your complaint relates to a Subject Access Request, please confirm the date of your request and the Data Subject it concerned. If you have the SAR 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.

23. 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 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, c)**

- 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,e)**
- 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,a)**
- If you give your consent, you may change your mind at any time.
- 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 h)** or to provide you with equal opportunities and treatment **(Article 9,g)** We will also use this information where you have given us permission to do so **(Article9,a)**.There may also be circumstances where we need to use your information in relation to legal claims **(Article 9 f)** , or to protect your vital interests and where you are unable to provide your consent **(Article 9 c)**.

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.

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 you 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. The school does 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 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 General Data Protection Regulation which applies across the European Union (including in the United Kingdom) 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 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** compliance with a legal obligation and **Article 9 2 b** 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 1 b** 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 1 a and 9 2 a).**

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.

The Department for Education (DfE) collects and processes personal data relating to those who work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

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.

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 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

We are required to pass information about our school employees to the DfE under section 7 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.

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.

Data collection requirements

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.

Sharing by the Department for Education

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.

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

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.

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 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 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. We will process your personal data for the following reasons:

1. Where we are required by law **(Article 6,c)** , 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,e)** , 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, a)**

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.

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

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

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.

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

24. 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.

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 from to the Trust 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 GDPR just by talking about personal data, can I?

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

25. 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 GDPR 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 GDPR 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 Directors. • 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 GDPR practice and information governance in schools meets the required standard. • Ensuring that information governance is integrated to 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 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 Lead in School	• Raise awareness of Data Protection in the Academy. • Raise awareness of the Delta Data Protection and Retention Policies. • Report data breaches to the Delta 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 GDPR 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.