

Data Protection Policy

Academic Year 2022-2023



Version and Date		Action/Notes	Date Written	Date to be Reviewed
5.0	08.12.2020	Approved by Board of Trustees	Updated Dec 2020	1 Year – Dec 2021
6.0	13.07.2021	Approved by Board of Trustees	Updated July 2021	1 Year – July 2022
7.0	12.07.2022	Approved by Board of Trustees	Updated June 2022	1 Year – July 2023

1. Policy Statement and Objectives

1.1 The objectives of this Data Protection Policy are to ensure that the Connect Education Trust (the “Trust”) and its directors, local governors, members and employees are informed about, and comply with, their obligations under the data protection regulations.

1.2 Further information can be found at: <https://ico.org.uk/for-organisations/guide-to-data-protection/>

1.3 The Trust is a Multi Academy Trust with individual academies and is the Data Controller for all the Personal Data processed by its schools/academies and by the central services of the Trust.

1.4 Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner. This personal information is collected by the academies within the Trust but also by the central team who work for the Trust.

1.5 The type of information that we may be required to handle include details of job applicants, current, past and prospective employees, pupils, parents/ carers and other members of pupils’ families, trustees, governors, members, suppliers and other individuals that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the data protection regulations. The regulations impose restrictions on how we may use that information.

1.6 This policy does not form part of any employee’s contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the data protection regulations may expose the Trust to enforcement action by the Information Commissioner’s Office (ICO) or fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Trust’s employees. At the very least, a breach of the regulations could damage our reputation and have serious consequences for the Trust and for our stakeholders.

2. Status of the Policy

2.1 This policy has been approved by the Board of Trustees. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3. Data Protection Officer

3.1 The Data Protection Officer (the “DPO”) is responsible for advising the Trust on compliance with the data protection regulations and with this policy. This work is carried out by an external company, Ex Cathedra Solutions Limited, and the designated DPO is Steve Durbin, Director, contactable at connectdpo@excathedra.solutions.

3.2 In addition, a 'link' person will be appointed at each academy within the Trust and will report to the DPO on matters relating to data protection compliance, to be known as the School Data Protection Lead.

3.3 Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

3.4 The DPO will play a major role in embedding essential aspects of the regulations into the Trust's culture, from ensuring the data protection principles are respected to preserving data subject rights, recording data processing activities and ensuring the security of processing.

3.5 The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data.

3.6 Since the DPO service is outsourced, the company is responsible for providing a suitable DPO, and as such the current requirements to ensure the above are:

3.6.1 senior management support;

3.6.2 official communication of the designation of the DPO to make known existence and function within the organisation;

3.6.3 access to other services, such as HR, IT and security, who should provide support to the DPO;

3.6.4 access to the "highest level of the organisation" in order to provide reporting to that level of compliance and issues;

3.7 Should the DPO service come back in house, the regulations require that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

3.7.1 senior management support;

3.7.2 time for DPOs to fulfil their duties;

3.7.3 adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;

3.7.4 official communication of the designation of the DPO to make known existence and function within the organisation;

3.7.5 access to other services, such as HR, IT and security, who should provide support to the DPO;

3.7.6 continuous training so that DPOs can stay up to date with regard to data protection developments;

3.2.7 where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;

3.7.8 whether the Trust should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

3.7.9 The DPO is responsible for advising the Trust on its processing operations and whether they adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the Trust must ensure the independence of the DPO.

3.7.10 The Trust will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the board of directors.

3.7.10 The requirement that the DPO reports directly to the board of directors ensures that the Board of Trustees are made aware of the pertinent data protection issues. In the event that the Trust decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the board of directors and to any other decision makers.

3.7.11 A DPO appointed internally by the Trust is permitted to undertake other tasks and duties for the organisation, but these must not result in a conflict of interests with his or her role as DPO. It follows that any conflict of interests between the individual's role as DPO and other roles the individual may have within the organisation impinge on the DPO's ability to remain independent.

3.7.12 In order to avoid conflicts the DPO cannot hold another position within the organisation that involves determining the purposes and means of processing personal data.

3.10 If you consider that the policy has not been followed in respect of Personal Data about yourself or others you should raise the matter with the DPO.

4. Definition of Terms

4.1 **Biometric Data** means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images; (UK GDPR Article 9)

4.2 **Consent of the Data Subject** means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her; (UK GDPR Article 7)

4.3 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems or other media such as CCTV;

4.4 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data; (UK GDPR Article 4)

4.5 **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; (UK GDPR Article 4)

4.6 **Data Users** include employees, volunteers, trustees [and local governors] whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;

4.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller; (UK GDPR Article 4)

4.8 **Parent** has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

4.9 **Personal Data** means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (UK GDPR Article 4)

4.10 **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 transmitted, stored or otherwise processed; (UK GDPR Article 4)

4.11 **Data Protection by Design and Default** means implementing appropriate technical and organisational measures in an effective manner to ensure that personal data is correctly protected; (UK GDPR Article 25)

4.12 **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (UK GDPR Article 4)

4.13 **Special Category Personal Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; (UK GDPR Article 9)

5. Data Protection Principles

5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. (UK GDPR Article 5). These provide that Personal Data must be:

5.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

5.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

5.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

5.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the data protection regulations in order to safeguard the rights and freedoms of individuals; and

5.1.6 Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Processed Lawfully, Fairly And In A Transparent Manner

6.1 The data protection regulations are intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the Trust), who the Data Controller's representative is (in this case the DPO), the purpose for which the data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

6.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include (UK GDPR Article 6):

6.2.1 where we have the Consent of the Data Subject;

6.2.2 where the processing is required for a contract to which the data subject is a party

6.2.2 where it is necessary for compliance with a legal obligation on the controller;

6.2.3 where processing is necessary to protect the vital interests of the Data Subject or another person;

6.2.4 where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

6.3 Purpose Limitation

6.3.1 Personal data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the regulations. This means that Personal Data must not be collected for one purpose and then used for another.

6.3.2 If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs. Personal data only relates to a 'living' individual.

6.4 Special Category Personal Data

6.4.1 The Trust will be processing Special Category Personal Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Special Category Personal Data.

6.4.2 When Special Category Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 6.2 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

6.4.2.1 the Data Subject's explicit consent to the processing of such data has been obtained

6.4.2.2 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

6.4.2.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

6.4.2.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

6.4.3 The Trust recognises that in addition to Special Category Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Special Category Personal Data.

6.5 Biometric Data

6.5.1 Academies in the Trust may process Biometric Data as part of an automated biometric recognition system, for example, for cashless catering or photo ID card systems where a pupil's photo is scanned automatically to provide him or her with services. Biometric Data is a type of Special Category Personal Data.

6.5.2 Where Biometric Data relating to pupils is processed, the relevant academy must ensure that each parent of a child is notified of the school's intention to use the child's Biometric Data and obtain the written consent of at least one parent before the data is taken from the pupil and used as part of an automated biometric recognition system. An academy must not process the Biometric Data if a pupil under 18 years of age where:

6.5.2.1 the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;

6.5.2.2 no Parent has Consented in writing to the processing; or

6.5.2.3 a Parent has objected in writing to such processing, even if another Parent has given written Consent.

6.5.3 Academies must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system and ensure that pupils not using the system are not disadvantaged by doing so. The Trust will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.

6.5.4 The Trust and/ or the relevant academies must obtain the explicit Consent of staff, trustees, local governors, members or other Data Subjects before Processing their Biometric Data.

6.6 Criminal convictions and offences

6.6.1 There are separate safeguards in the data protection regulations for Personal Data relating to criminal convictions and offences.

6.6.2 It is likely that the Trust and its academies will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff, trustees and local governors or due to information which we may acquire during the course of their employment or appointment.

6.6.3 In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. This information is not routinely collected and is only likely to be processed by the Trust in specific circumstances, for example, if a child protection issue arises or if a parent/ carer is involved in a criminal matter.

6.6.4 Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

6.7 Transparency

6.7.1 One of the key requirements of the data protection regulations relates to transparency. This means that the Trust must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

6.7.2 One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The Trust has developed privacy notices for the following categories of people:

- Pupils
- Parents
- Staff and contractors
- Trustees/ Governors

6.7.7 The Trust wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Trust employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to Academy premises or if we ask people to complete forms requiring them to provide their Personal Data.

6.7.8 We will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

6.7.9 We will advise parents that when taking photos or videos it must be for their personal use only and not shared on social media.

6.8 Consent

6.8.1 The Trust must only process Personal Data on the basis of one or more of the lawful bases set out in the data protection regulations, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

6.8.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.8.3 In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to obtain Consent from the Parent(s).

In the event that we require Consent for Processing Personal Data about pupils aged 13 or over, we will require the Consent of the pupil although, depending on the circumstances, academies should consider whether it is appropriate to inform Parents about this process.

Consent is likely to be required if, for example, an academy wishes to use a photo of a pupil on its website or on social media. Consent is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent if the pupil is aged under 13. When relying on Consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

6.8.4 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.8.5 Evidence and records of Consent must be maintained so that the Trust can demonstrate compliance with Consent requirements.

7. Specified, Explicit and Legitimate Purposes

7.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any data which is not necessary for that purpose should not be collected in the first place.

7.2 The Trust will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

8. Adequate, Relevant and Limited to What Is Necessary

8.1 The Trust will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

8.2 In order to ensure compliance with this principle, the Trust will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

8.3 Trust employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a school functions and we should not collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes. On forms requiring personal data, we will mark clearly what information is required by law.

8.4 The Trust will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis.

This means that the only members of staff, governors or trustees who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the Trust may adopt a layered approach in some circumstances, for example, members of staff, Trustees or members of the Local Education Committee may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Special Category Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

8.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the Trust's data retention guidelines.

9. Accurate and, Where Necessary, Kept Up To Date

9.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9.2 If a Data Subject informs the Trust of a change of circumstances their records will be updated as soon as is practicable. Schools are able to produce a staff and parent report from their Schools Management Information System (MIS) to evidence data accuracy. Staff are advised by Headteachers to notify their HR Officer of any change to their personal data.

9.3 Where a Data Subject challenges the accuracy of their data, the Trust will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer OR Chair of Local Governors on the Local Governing Body or the Board of Trustees for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

9.4 Notwithstanding paragraph 9.3, a Data Subject continues to have rights under the data protection regulations and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 9.3 has been followed.

10. Data to be kept for no longer than is necessary for the purposes for which the Personal Data are processed

10.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

10.2 It is the duty of the Trust, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The Trust has a retention schedule for all data. The Management of Records Guidance and Information document evidences how effective management is achieved and audited.

11. Data to be processed in a manner that ensures appropriate security of the Personal Data

11.1 The Trust has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

11.2 The regulations requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

11.3 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, and the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

11.4 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Special Category Personal Data from loss and unauthorised access, use or disclosure.

11.5 Data Users must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our policy and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the relevant standards to protect Personal Data.

11.6 It is the responsibility of all members of staff, trustees and local governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher of the relevant Academy or the DPO.

11.8 Trustees and Local Governors

11.8.1 Trustees and Local Governors are likely to process Personal Data when they are performing their duties, for example, if they are dealing with employee issues, pupil exclusions or parent complaints. Trustees and

Governors should be trained on the Trust's data protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

11.8.1.1 Ensure that Personal Data which comes into their possession as a result of their Trustee or Local Governor duties is kept secure from third parties, including family members and friends;

11.8.1.2 using a Trust email account for any Trust-related communications;

11.8.1.3 Ensuring that any Trust-related communications or information stored or saved on an electronic device or computer is encrypted and protected by password, PIN or biometric access control;

11.8.1.4 Taking appropriate measures to keep Personal Data secure, which includes ensuring that hard copy documents are securely locked away so that they cannot be access by third parties

12. Data Subjects' Rights

12.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

12.1.1 withdraw Consent to Processing at any time;

12.1.2 receive certain information about the Data Controller's Processing activities;

12.1.3 request access to their Personal Data that we hold;

12.1.4 prevent our use of their Personal Data for direct marketing purposes;

12.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

12.1.6 restrict Processing in specific circumstances;

12.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

12.1.8 request a copy of an agreement under which Personal Data is transferred outside of the UK;

12.1.9 object to decisions based solely on Automated Processing, including profiling (Automated Decision Making);

12.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

12.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

12.1.12 make a complaint to the supervisory authority (the ICO); and

12.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

12.2 We are required to verify the identity of an individual requesting data under any of the rights listed above.

Members of staff should not allow third parties to persuade them into disclosing Personal Data without proper authorisation.

13. Providing Information over the Telephone

13.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any Personal Data held by the Trust whilst also applying common sense to the particular circumstances. In particular they should:

13.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

13.1.2 Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

13.1.3 Refer to their line manager or the DPO for assistance in difficult situations. No-one should feel pressurised into disclosing personal information.

14. Authorised Disclosures

14.1 The Trust will only disclose data about individuals if one of the lawful bases apply.

14.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The Trust and its academies will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

14.2.1 Local Authorities

14.2.2 the Department for Education

14.2.3 the Education & Skills Funding Agency

14.2.4 the Disclosure and Barring Service

14.2.5 the Teaching Regulation Agency

14.2.6 the Teachers' Pension Service

14.2.7 the Local Government Pension Scheme which is administered by the London Borough of Enfield.

14.2.8 our external HR provider

14.2.9 our external payroll provider

14.2.10 our external IT Provider

14.2.11 our Asset Management provider

14.2.12 our Accountants

14.2.13 our Auditors

14.2.14 other external Educational providers of services

14.2.15 HMRC

14.2.16 the Police or other law enforcement agencies

14.2.17 our legal advisors and other consultants

14.2.18 insurance providers/ the Risk Protection Arrangement

14.2.19 Occupational Health Advisors

14.2.20 exam boards

14.2.21 the Joint Council for Qualifications;

14.2.22 NHS health professionals including educational psychologists and school nurses;

14.2.23 Education Welfare Officers;

14.2.24 Courts, if ordered to do so;

14.2.25 Prevent teams in accordance with the Prevent Duty on schools;

14.2.26 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;

14.2.27 confidential waste collection companies

14.2.28 Other suppliers of services

14.3 Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches.

14.4 The regulations require Data Controllers to have a written contract in place with Data Processors which must include specific responsibilities on the processor. It will be the responsibility of the Academy entering into the contract to ensure that contracts comply with this, which is documented in our Data Processing Agreements Policy.

Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

14.5 In some cases, Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the regulations, including responsibility for any Personal Data Breaches, onto the Trust. In these circumstances, the member of staff dealing with the contract should contact the DPO for further advice before agreeing to include such wording in the contract.

15. Reporting a Personal Data Breach

15.1 The regulations require that we record ALL personal data breaches, no matter how minor. This includes near misses.

15.2 The regulations require Data Controllers to notify any Personal Data Breach to the ICO where there is a “significant risk to the rights and freedoms of the data subject(s)”.

15.3 A notifiable Personal Data Breach must be reported to the ICO without undue delay and where feasible within 72 hours unless the data breach is unlikely to result in a risk to the individuals.

15.4 If the breach is likely to result in high risk to affected Data Subjects, we must inform them without delay.

15.4 The DPO, or the nominated deputy DCEO/CFO, will assist in deciding whether to report a Personal Data Breach to the ICO. The DPO is contactable out of hours and during school holidays for this purpose.

15.5 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

15.6 The Trust recognises that as our academies are closed or have limited staff available during school holidays, there will be times when our ability to respond to a Personal Data Breach promptly and within the relevant timescales will be affected. We will consider any proportionate measures that we can implement to mitigate the impact this may have on Data Subjects.

15.7 If a member of staff, trustee or local governor knows or suspects that a Personal Data Breach has occurred, our Security Incident Response Plan must be followed. In particular, the DPO or DCEO/CFO must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

16. Accountability

16.1 The Trust must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Trust is responsible for, and must be able to demonstrate, compliance with the data protection principles.

16.2 The Trust must have adequate resources and controls in place to ensure and to document compliance including:

16.2.1 appointing a suitably qualified DPO (where necessary) and an executive team accountable for data privacy;

16.2.2 implementing Data Protection by Design and Default when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;

16.2.3 integrating data protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;

16.2.4 regularly training Trust employees, trustees and [governors] on the GDPR, this Data Protection Policy, related policies and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The Trust must maintain a record of training attendance by Trust personnel; and

16.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record Keeping

17.1 The regulations require us to keep full and accurate records of all our Data Processing activities.

17.2 We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

17.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. Training and Audit

18.1 We are required to ensure all Trust personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

18.2 Members of staff must attend all mandatory data privacy related training, which will be evidenced on the Central Training Spreadsheet.

19. Data Protection by Design and Default and Data Protection Impact Assessment (DPIA)

19.1 We are required to implement Data Protection by Design and Default measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

19.2 This means that we must assess what measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

19.2.1 the state of the art;

19.2.2 the cost of implementation;

19.2.3 the nature, scope, context and purposes of Processing; and

19.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

19.3 We are also required to conduct DPIAs in respect to high risk Processing. We have carried out a wider DPIA into our school's general processing and controls, but where specific additional risks are raised, this will require a local DPIA.

19.4 The Trust and schools must be law contact the DPO in a timely manner if any new or changed processing is planned. The DPO will advise on the requirements of the DPIA and their advice must be considered. If rejected, the fact of this rejection and reasons for doing so must be recorded.

20. CCTV

20.1 The Trust and its academies use CCTV in locations around some of their sites. This is to:

20.1.1 protect the academy buildings and their assets;

20.1.2 increase personal safety and reduce the fear of crime;

20.1.3 support the Police in a bid to deter and detect crime;

20.1.4 assist in identifying, apprehending and prosecuting offenders;

20.1.5 provide evidence for the Trust to use in its internal investigations and/ or disciplinary processes in the event of behaviour by staff, pupils or other visitors on the site which breaches or is alleged to breach the Trust's policies;

20.1.6 protect members of the school community, public and private property; and

20.1.7 assist in managing the academy.

20.2 Please refer to the Trust's CCTV Policy for more information.

21. Policy Review

21.1 It is the responsibility of the directors to facilitate the review of this policy on a regular basis. Recommendations for any amendments should be discussed with the DPO.

21.2 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

22. Enquiries

Further information about the School's Data Protection Policy is available from the DPO.

General information about the regulations can be obtained from the Information Commissioner's Office.

This policy will be reviewed on an annual basis by the Board of Trustees.