Data Protection Policy

ENFIELD
LEARNING TRUST

BE INCLUDED
BE CONNECTED

Version and Date		Action/Notes	Date Written	Date to be Reviewed
3.0	31.03.2020	Approved by Board of Trustees	January 2020	2 Years – January 2022
4.0	02.10.2020	Approved by Board of Trustees	Updated Oct 2020	2 Years – Oct 2022

Policy Statement and Objectives

1.1 The objectives of this Data Protection Policy are to ensure that Enfield Learning Trust (the "Trust") and its directors, local governors, members and employees are informed about, and comply with, their obligations under the General Data Protection Regulation ("the GDPR") and other data protection legislation

1.2 Further information can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

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 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, local 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 GDPR and other legislation. The GDPR imposes 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 GDPR 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 GDPR 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**

The Data Protection Officer (the "DPO") is responsible for ensuring the Trust is compliant with the GDPR and with this policy. This post is held by Steve Durbin, Director of Ex Cathedra Solutions (steve.durbin@excathedra.solutions). 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

Academy Data Protection Lead. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

3.1 The DPO will play a major role in embedding essential aspects of the GDPR 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.

3.2 The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the GDPR requires 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:

3.2.1 senior management support;

3.2.2 time for DPOs to fulfil their duties;

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

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

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

3.2.6 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;

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

3.3 The DPO is responsible for ensuring that the Trust's Processing operations 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.

3.4 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.

3.5 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.

3.6 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 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. Senior management positions such as Chief Executive Officer, Chief Financial Officer, Head of Marketing, Head of IT or Head of Human Resources positions are likely to cause conflicts. Some other positions may involve determining the purposes and means of processing, which will rule them out as feasible roles for DPOs.

3.8 In the light of this and in the event that the Trust decides to appoint an internal DPO, the Trust will take the following action in order to avoid conflicts of interests:

3.8.1 identify the positions incompatible with the function of DPO;

3.8.2 draw up internal rules to this effect in order to avoid conflicts of interests which may include, for example, allocating some of the DPO's other duties to other members of staff, appointing a deputy DPO and / or obtaining advice from an external advisor if appropriate;

3.8.3 include a more general explanation of conflicts of interests;

3.8.4 declare that the DPO has no conflict of interests with regard to his or her function as a DPO, as a way of raising awareness of this requirement.

3.8.5 Include safeguards in the internal rules of the organisation and ensure that the job specification for the position of DPO or the service contract is sufficiently precise and detailed to avoid conflicts of interest.

3.9 External service providers will have different considerations over conflicts of interests, such as whether other advice provided to the organisation (for example, relating to the organisation's use of personal data) would affect their independence in the role of DPO.

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;

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;

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.

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.

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;

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;

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;

4.11 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR;

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;

4.13 **Sensitive 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.

5. Data Protection Principles

5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. 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 GDPR 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 GDPR is 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:

6.2.1 where we have the Consent of the Data Subject;

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

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 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 Act. This means that Personal Data must not be collected for one purpose and then used for another. 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 Sensitive Personal Data

6.4.1 The Trust will be processing Sensitive 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 Sensitive Personal Data.

6.4.2 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 6.3 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 Sensitive 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 Sensitive 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 Sensitive 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. 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 GDPR 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 GDPR 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:

6.7.3 Pupils

6.7.4 Parents

6.7.5 Staff

6.7.6 Trustees/ Local 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 GDPR, 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 unlikely to be 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 is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent is 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 will not be shared regularly without consent, and that we only do so when we have to.

6.8.5 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.

6.8.6 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Often, we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data.

6.8.7 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 the 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.

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 Sensitive 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 GDPR 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 DPO, 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 GDPR 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, 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 Sensitive 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 GDPR and relevant standards to protect Personal Data **(see appendix 2)**.

11.6 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

11.6.1 **Confidentiality** means that only people who are authorised to use the data can access it.

11.6.2 **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.

11.6.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

11.7 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 password protected and encrypted;

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. **Processing in Line with 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 EEA;

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. **Dealing with Subject Access Requests**

13.1 The GDPR extends to all Data Subjects a right of access to their own Personal Data. A Subject Access Request (SAR) can be submitted in any form to the Headteacher from a Data Subject for information that we hold about them. Previous staff, ex -employees to contact the HR Officer.

13.2 It is important that all members of staff are able to recognise that a written request made by a person for their own information is likely to be a valid Subject Access Request, even if the Data Subject does not specifically use this phrase in their request or refer to the GDPR. In some cases, a Data Subject may mistakenly refer to the "Freedom of Information Act" but this should not prevent an Academy or the Trust from responding to the request as being made under the GDPR, if appropriate. Some requests may contain a combination of a Subject Access Request for Personal Data under the GDPR and a request for information under the Freedom of Information Act 2000 ("FOIA"). Requests for information under the FOIA must be dealt with promptly and in any event within 20 school days.

13.3 Any member of staff who receives a written request of this nature must immediately forward it to the DPO as the statutory time limit for responding is **one calendar month**. Under the Data Protection Act 1998 (DPA 1998), Data Controllers previously had 40 calendar days to respond to a request. We don't think we will need to extend the response time, which we're able to do when requests are complex. However, if it becomes clear that we do need to extend the response period by up to 2 months, we will let you know.

13.4 As the time for responding to a request does not stop during the periods when an academy is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing the following measures: In the absence of the Data Protection Officer the Deputy CEO/CFO will respond to any written request.

13.5 A fee may no longer be charged to the individual for provision of this information (previously a fee of £10 could be charged under the DPA 1998). Please See the latest ICO guidance for further information. The contact details are in clause 1.2.

13.6 The Academy or central services of the Trust may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

13.7 In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place.

13.8 Requests from pupils who are considered mature enough to understand their rights under the GDPR will be processed as a subject access request as outlined below and the data will be given directly to the pupil (subject to any exemptions that apply under the GDPR or other legislation). [As the age when a young person is deemed to be able to give Consent for online services is 13, we will use this age as a guide for when pupils may be considered mature enough to exercise their own subject access rights]. In every case it will be for the Trust, as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

13.9 Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

13.10 Requests from Parents in respect of their own child will be processed as requests made on behalf of the Data Subject (the child) where the pupil is aged under 13 (subject to any exemptions that apply under the Act or other legislation). If the Parent makes a request for their child's Personal Data and the child is aged 13 or older and/ or the Trust considers the child to be mature enough to understand their rights under the GDPR, the Trust shall ask the pupil for their Consent to disclosure of the Personal Data if there is no other lawful basis for sharing the Personal Data with the Parent (subject to any enactment or guidance which permits the Trust to disclose the Personal Data to a Parent without the child's Consent). If Consent is not given to disclosure, the Trust shall not disclose the Personal Data if to do so would breach any of the data protection principles.

13.11 It should be noted that the Education (Pupil Information) (England) Regulations 2005 do not apply to academies so the rights available to parents in those Regulations to access their child's educational records are not applicable to academies in the Trust. Instead, requests from Parents for Personal Data about their child must be dealt with under the GDPR (as outlined above). This is without prejudice to the obligation on the Trust in the Education (Independent School Standards) Regulations 2014 to provide an annual report of each registered pupil's progress and attainment in the main subject areas taught to every parent (unless they agree otherwise in writing).

13.12 Following receipt of a subject access request, and provided that there is sufficient information to process the request, an entry should be made in the Trust's Subject Access log book, showing the date of receipt, the Data Subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date for supplying the information (not more than one calendar month from the request date). Should more information be required to establish either the identity of the Data Subject (or agent) or the type of data requested, the date of entry in the log will be date on which sufficient information has been provided.

13.13 Where requests are "manifestly unfounded or excessive", in particular because they are repetitive, the Trust can:

13.13.1 charge a reasonable fee taking into account the administrative costs of providing the information; or

13.13.2 refuse to respond.

13.14 Where we refuse to respond to a request, the response must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month. Members of staff should refer to any guidance issued by the ICO on Subject Access Requests and consult the DPO before refusing a request. The DPA and latest ICO guidance have set out the reasons for refusing a subject access request more clearly and includes refusal if:

- Another person's personal data cannot be reasonably anonymised, and we do not have the other person's consent as it would be unreasonable to proceed without it

- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references or exam scripts

13.15 Certain information may be exempt from disclosure so members of staff will need to consider what exemptions (if any) apply and decide whether you can rely on them. For example, information about third parties may be exempt from disclosure. In practice, this means that you may be entitled to withhold some documents entirely or you may need to redact parts of them. Care should be taken to ensure that documents are redacted properly. Please seek further advice or support from the DPO if you are unsure which exemptions apply.

13.16 In the context of an Academy a subject access request is normally part of a broader complaint or concern from a Parent or may be connected to a disciplinary or grievance for an employee. Members of staff should therefore ensure that the broader context is taken into account when responding to a request and seek advice if required on managing the broader issue and the response to the request.

13.17 Upon refusal of a SAR, individuals can seek to enforce their subject access right through the courts.

14. **Providing Information over the Telephone**

14.1 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:

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

14.1.2 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.

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

15. **Authorised Disclosures**

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

15.2 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:

15.2.1 Local Authorities

15.2.2 the Department for Education

15.2.3 the Education & Skills Funding Agency

15.2.4 the Disclosure and Barring Service

15.2.5 the Teaching Regulation Agency

15.2.6 the Teachers' Pension Service

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

15.2.8 our external HR provider

15.2.9 our external payroll provider

15.2.10 our external IT Provider

15.2.11 our Asset Management provider

15.2.12 our Accountants

15.2.13 our Auditors

15.2.14 other external Educational providers of services

15.2.15 HMRC

15.2.16 the Police or other law enforcement agencies

15.2.17 our legal advisors and other consultants

15.2.18 insurance providers/ the Risk Protection Arrangement

15.2.19 Occupational Health Advisors

15.2.20 exam boards

15.2.21 the Joint Council for Qualifications;

15.2.22 NHS health professionals including educational psychologists and school nurses;

15.2.23 Education Welfare Officers;

15.2.24 Courts, if ordered to do so;

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

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

15.2.27 confidential waste collection companies

15.2.28 Other suppliers of services

15.3 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.

15.4 The GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is Processed ("GDPR clauses"). A summary of the GDPR clauses is set out in **Appendix 1**. It will be the responsibility of the Academy entering into the contract to ensure that the GDPR clauses have been added to the contract with the Data Processor. 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.

15.5 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 GDPR, 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.

16. **Reporting a Personal Data Breach**

16.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject.

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

16.3 If the breach is likely to result in high risk to affected Data Subjects, the GDPR, requires organisations to inform them without undue delay.

16.4 It is the responsibility of the DPO, or the nominated deputy DCEO/CFO, to decide whether to report a Personal Data Breach to the ICO.

16.5 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.

16.6 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.

16.7 If a member of staff, trustee or local governor knows or suspects that a Personal Data Breach has occurred, our Security Incident Response Plan **(see appendix 3)** 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.

17. Accountability

17.1 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.

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

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

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

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

17.2.4 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

17.2.5 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.

18. Record Keeping

18.1 The GDPR requires us to keep full and accurate records of all our Data Processing activities.

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

18.3 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.

19. **Training and Audit**

19.1 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.

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

20. **Privacy by Design and Data Protection Impact Assessment (DPIA)**

20.1 We are required to implement Privacy by Design 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.

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

20.2.1 the state of the art;

20.2.2 the cost of implementation;

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

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

20.3 We are also required to conduct DPIAs in respect to high risk Processing.

20.4 The Trust and its academies should conduct a DPIA and discuss your findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including:

20.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

20.4.2 Automated Processing including profiling and automated decision making (ADM);

20.4.3 large scale Processing of Sensitive Data; and

20.4.4 large scale, systematic monitoring of a publicly accessible area.

20.5 We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to pupils. If our processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

20.6 A DPIA must include:

20.6.1 a description of the Processing, its purposes and the Trust's legitimate interests if appropriate;

20.6.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

20.6.3 an assessment of the risk to individuals; and

20.6.4 the risk mitigation measures in place and demonstration of compliance.

21. **CCTV**

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

21.1.1 protect the academy buildings and their assets;

21.1.2 increase personal safety and reduce the fear of crime;

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

21.1.4 assist in identifying, apprehending and prosecuting offenders;

21.1.5 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;

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

21.1.7 assist in managing the academy.

21.2 Please refer to the Trust's CCTV Guidance & Information for more information **(see appendix 4)**

22. **Policy Review**

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

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

23. **Enquiries**

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

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

Appendix 1 – GDPR Clauses

The GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))

2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))

3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)

4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object. (Art. 28(2) Art. 28(3)(d))

5. The Processor must ensure it flows down the GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))

6. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3)(e))

7. The Processor must assist the Data Controller with their security and data breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))

8. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))

9. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3)(g))

10. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))

11. The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3))

The GDPR Regulation: Data Protection Principles

1. Personal data shall be processed fairly and lawfully and in a transparent manner in relations to individuals.

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;

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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. 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 GDPR in order to safeguard the rights and freedoms of individuals;

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."

7. The controller to ensure all Contracts are GDPR compliant. This can be evidence using the Suppliers Contract Checklist.

8. "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."

This is not a full explanation of the principles, for further information refer to the GDPR Regulations.

Appendix 2

Data Security

- Personal data held in paper form is kept in locked cabinets and is only taken off school premises with the permission of the Headteacher, on the understanding that it be securely stored.
- Personal data should always be locked away at the end of every day and should not be left visible on desks, noticeboards, etc. at any time.
- Protectively mark documents (electronic or paper) that are sensitive
- Never just 'forward' sensitive documents/data out of one email system to another email system without protecting the data. Care should be taken to ensure the email is correctly addressed.
- Do not use personal computer systems or personal email addresses; these may not have adequate security protection.
- If sending through post - double bag and mark the inside bag confidential/sensitive. Consider using courier / recorded post if particularly sensitive.
- Equipment must be disposed of by following WEEE (Waste Electrical and Electronic Directive). Ensure the disposer/recycler securely wipes data to ICO standards on all hardware (include photocopiers).
- All computers are 'on the network' or synchronised with it regularly, so kept up to date with protection software (anti-virus etc.,) so data is not put at risk.
- Sensitive documents or photographs stored by staff on the school network, must be in folders in an area restricted to relevant staff only.
- All devices (laptops, external hard drives) are actively encrypted if used for storing sensitive data.
- Back-up is daily and stored in encrypted format. If physical tapes are used they must be stored in a secure, fire-proof safe. Periodically, check back-ups are correctly working. Preferably, use remote, secure back-up, for disaster recovery.
- All devices are set-up with auto-lock after 'X' minutes on relevant devices to secure them if they are left idle.
- Gmail or Egress are used to exchange sensitive data and documents, e.g. for sending references or documents about named children.
- Laptops and computers are password protected
- Regular password changes where possible. (Normal recommendation is every 90 days.)
- Recommended email, online platforms or portals and remote access to school or web hosted resources are in place.
- Personal data held on a computer must be password protected or encrypted and regularly backed up.
- Personal information held on a memory drive must be kept in a locked filing cabinet, drawer or safe.
- Child Protection records are kept in a locked cabinet – access is restricted to the Senior Leadership Team.
- Sensitive data should never be stored off site.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- Personal Data re: school census must always be transferred securely via Egress, collect or S2S
- Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
- Management of user accounts - Headteachers should determine what rights and privileges users need to effectively perform their duties and implement.
    - **Establish effective account management processes:** Manage user accounts from creation, through-life and eventually revocation when a member of staff leaves or changes role. Redundant accounts, perhaps provided for temporary staff or for testing, should be removed or suspended when no longer required.
    - A corporate password should be developed that seeks an effective balance between security. Some accounts an additional authentication factor (such as a …) may be appropriate.
    - **Limit user privileges:** Users should be provided with the reasonable minimum rights and permissions to systems
- Training will be given to all groups of staff to ensure the Trust is compliant and risk rating is low.

- Mobile telephones are password protected. Users must download the tracker system Find My iPhone which wipes data if lost.
- Email security – when selecting your password, you need to ensure you choose a strong password. The ICO guidance is the password must be at least 10 characters long, and not reusing passwords from other sites.
- Check your email setting and report scams, spam and phishing to your ICT lead/DPO.
- Spam and risks from viruses you must ensure that all machines are configured to run the latest anti-virus software as approved.
- Removable media - do not use removable media as a default mechanism to store or transfer information. Under normal circumstances information should be stored on corporate systems and exchanged using appropriately protected mechanisms.
- Homework environment – teachers need to check who has access (admin rights), monitoring what is being uploaded and the companies, security- agreement.
- Wireless internet -avoid using the default password or guest password to join the network and ensure you encrypt your data.
- Appropriate safeguards are in place when transferring data outside of the European Economic Area
- When disposing of PC's/servers all data must be securely disposed of when no longer required. An automatic process must exist to permanently delete on-line data, when no longer required and you should ensure that you receive a certificate of the company who is disposed any hardware.
- Any lost device needs to be report immediately to the Headteacher, or the ELT Chief Operations Officer and a report of what data was stored and if the item has a tracking system in place. The lost item must also be entered onto the assets management system
- CCTV hard drives must be password protected and kept in a lock room. Images captured by the system must be caught securely therefore access to the room must be controlled.
- The firewall prevents **unauthorised access** to or from a private computer network. Firewalls are frequently used to prevent **unauthorised** Internet users from accessing private networks connected to the Internet.
- Patch management - we only use licensed and supported software and install software updates and security patches in a timely manner.
- Mobile devices - signed paperwork for mobile devices are retained by ELT HR/Finance. All assets are password protected. A firewall is installed on Laptops to prevent **unauthorised access** to or from a private computer network. Firewalls are frequently used to prevent **unauthorised** Internet users from accessing private networks connected to the Internet.

Appendix 3

Security Incident Reporting Information and Plan

1. Purpose

1.1 The purpose of this document is to describe the procedures for identifying, reporting, responding to, and learning from loss of information and information systems e.g. laptops, USBs and hard copy files / documents.

2. Scope

2.1 This procedure is applicable to all aspects of the Trusts operations whether electronic, non-electronic, personnel, premises or infrastructure

3. Overview

3.1 All systems and activities will be subject to formal incident recording and escalation procedures.

3.2 Incident recording will be used to log all unusual events. The mechanism will include what happened, what was done and final solution.

3.3 The objective of Security Incident Reporting and Management is to detect, investigate and resolve any actual, suspected or potential breaches of information security, and to take action that will avoid, or reduce the impact or probability of a further similar reoccurrence.

3.4 A security incident is an event which causes or has potential to cause:

- loss of system or information availability
- disclosure of confidential information, whether electronic or paper, or any other form including conversation
- corruption of information
- disruption of activity
- financial loss
- legal action.

3.5 Examples of incidents could include activity such as:

- the unauthorised use of a system for the processing or storage of data
- loss of removable media (USB Stick, Disc etc) and portable equipment (Laptops/ PCs)
- loss of paper files containing sensitive data.

3.6 The following should be established as rapidly as possible:

- when the incident occurred; whether a near miss or an actual incident.
- when the incident was discovered
- details of the person reporting the incident;
- what data and data media involved;
- who is involved (e.g. individuals, schools);
- where the incident occurred;
- the sensitivity of the data and if personal data, the number of persons involved;
- whether the information and/or media was protectively marked and if so at what level;
- who is aware of the incident;
- whether and how the data might be used by a third party;
- the Information Asset Owner for the information involved;
- the immediate cause of the information loss e.g. breach, theft, misplaced, destroyed;
- the location of the information at the point of loss e.g. in the post, with a courier, in School/ Office;

- If in the post
- How was it sent?
- Was it double enveloped?
- Was the address verified?
- Where was it sent from?
- Was it double enveloped?

If with a courier

- From where was it collected?
- Was it sent with “track and trace”?
- Was it collected by the expected courier?
- Was the address verified?
- Was it double enveloped?

If from School/Office

- From where was it accessed/stole? (e.g. public areas, desk, drawer, filing cabinet, office)
- Was it protectively marked?
- If it was protectively marked, was it stored appropriately?

The crime number if the incident has been reported to the Police.

3.7 While each employee is personally responsible for ensuring that no security breaches occur as a result of their actions, everyone must be aware of their responsibility to report any potential, suspected or actual incident such as (security threats?), data loss, vulnerabilities, breaches, software or system failures to the Headteacher or ELT.

3.8 Security breaches caused knowingly by reckless behaviour, or non-compliance with Security Policies including the non-reporting of an incident, may result in disciplinary action.

4. Responsibilities

4.1 Users

- report any incidents promptly to the Headteacher or ELT
- provide further information or evidence when requested.

4.2 Information Asset Owner

- report all incidents to Headteacher or ELT
- complete Security Incident Report Form

4.3 Lead Data Protection (Headteacher)

- disseminate blank Security Incident Report Forms on request
- log and allocate reference for completed Security Incident Report forms
- report all incidents to Asset Business Manager / Data Protection Officer
- throughout the resolution period – keep the Incident Report Progress Record (spreadsheet) up to date
- maintain library of completed records

4.4 Headteacher

- allocate severity and priority to incident and agree resolution action plan
- monitor the resolution

- advise and involve other parties as appropriate (Chief Operations Officer, COO)
- review resolved incident and manage activities to avoid or reduce the probability of reoccurrence and the potential impact of future incidents
- approve closure of resolved incidents
- provide annual Process Owner's Report to MOD CIO

4.5 ICT Lead

- report data loss and hardware incidents to Headteacher

5. Procedure

5.1 This section describes procedure, but as every incident is different, common sense should be used to ensure that incidents are resolved with appropriate priority according to their severity.

5.2 Prompt action may be necessary to reduce the potential impact of an incident, so there may be times when an incident is resolved before it is recorded. If this occurs, an incident report form should be completed as soon as possible after the event.

5.3 It is important that every incident, however minor is recorded and follows this procedure to ensure that the probability of reoccurrence is avoided or reduced, and the impact of future incidents is minimised.

5.4 Recording

- Every reported incident will be recorded on a Security Incident report form (see Appendix A)
- Headteacher will allocate a Reference Number and record the details on the Incident Report Progress Record
- Headteacher will keep the records up to date as resolution progresses

5.5 Resolution

Once the incident has been recorded, it will be prioritised according to severity, which will be based upon the actual or potential impact of the incident upon the Agency's systems and information and will be categorised as:

- Critical (C)
- High (H)
- Medium (M)
- Low (L)

Resolution of the incident will be allocated to an individual or team, and an action plan will be produced with target resolution times. The resources used to resolve the incident will depend upon the identified severity level. For example, in the case of a Low severity "no action" may be an acceptable option if the resources required outweigh the impact.

5.6 Escalation

Every security incident that may have an impact on schools, pupils, staff or parents will be reported immediately to the COO and Asset Business Manager/DPO. If it is appropriate to do so the CEO & Deputy CEO/CFO will be made aware of the incident.

Personal Data Breach

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO the relevant supervisory authority, and you must do this within **72 hours of becoming aware of the breach**, where feasible.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay, keeping a record of any personal data breaches, regardless of whether you are required to notify.

On resolution of the incident, actions taken will be recorded on the Security Incident Report Form.

5.7 Review and Learning

All resolved incidents will be reviewed to ascertain whether there is a risk of reoccurrence. If there is no such risk the incident record will be closed. All potential vulnerabilities will be assessed, and appropriate action taken to ensure that the risk is kept to an acceptable level, implementing such controls as may be necessary.

- where appropriate risk registers will be updated.

5.8 Closure

Each incident will remain open until it has been satisfactorily resolved, documentation completed, and actions taken to avoid reoccurrence, or to ensure the impact of reoccurrence is at an acceptable level.

Closure will be approved by the Chief Operations Officer.

Appendix A - Security Incident Reporting Form

Please use this form to report any breach of security e.g. break in, theft, loss of laptop or data

Date of Incident:	Place of Incident:

Name of person reporting incident: (in block capitals)

Brief Description of Incident:

Brief Description of Any Action Taken (at time of discovery):

Date form sent to Headteacher:	Name of Headteacher: (in block capitals) Signature:

Overleaf for Headteacher Use

For Completion by Headteacher

Date Form Received: Date COO/DPO informed:	Incident Number:

Brief Description of Action taken:

Date of Follow up & Brief Description of Follow up Action:

Appendix 4

CCTV – Guidance & Information

1. Introduction

1.1 Some of the Enfield Learning Trust (ELT) sites use closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent the loss or damage to school property.

1.2 The system comprises of a number of fixed cameras.

1.3 Some CCTV's may have sound recording capability. If you capture sound recordings they should only be obtained when it is absolutely necessary and for this specific purpose. CCTV surveillance systems should not normally be used to record conversations between members of the public or members of staff as part of a working environment. Recording conversations is highly intrusive and unlikely to be justified and performance of a Data Protection Impact Assessment (DPIA) would identify this.

1.4 The CCTV system is owned and operated by the school and the deployment of which is determined by the school's leadership team.

1.5 The CCTV is monitored centrally from the school office by the, office staff, site staff and senior leadership team.

1.6 The introduction of, or changes to, CCTV monitoring will be subject to consultation with stakeholders.

1.7 The use of CCTV, and the associated images and any sound recordings, is covered by the GDPR 2018. This policy outlines the school's use of CCTV and how it complies with the regulation.

1.8 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the school data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

1.9 Any academy wishing to install CCTV will need to conduct a DPIA to help identify the most effective way to comply with the GDPR regulations and meet individuals' expectations of privacy.

1.10 CCTV system should have the ability to be switched on or off, if this is appropriate, so that recording of footage is not continuous. The system should also have the ability to stop capturing either footage and/or

sound recordings both of which should work independently of each other. Capturing both could be deemed excessive and you would need to demonstrate clearly the reasons for recording both and what legitimate grounds you are relying on to justify this.

1.11 CCTV recordings must be of a sufficient quality to be fit for their intended purpose and a regular check carried out to ensure that the date and time stamp recorded on images is accurate?

2. Statement of Intent

2.1 The school complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at: https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

2.2 CCTV warning signs will be clear and prominently placed, including school gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV **(see appendix 4).** In areas where CCTV is used, the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

2.3 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3. Siting the Cameras

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The School will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

3.2 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

3.3 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. Covert Monitoring

4.1 The Trust may, in exceptional circumstances, set up covert monitoring. For example:

ii) Where there is good cause to suspect that an illegal or unauthorised action(s) is taking place, or where there are grounds to suspect serious misconduct;

iii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances, authorisation must be obtained from a member of the Executive Leadership Team of the Trust.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

5. Storage and Retention of CCTV images

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All recordings from the CCTV system will be stored securely i.e. password protected.

5.3 CCTV recordings are deleted when they no longer serve a purpose.

5.4 Individuals must be notified with fair processing information including letting them know when they are in an area where a surveillance system is in operation and their right to access their recordings/ images?

6. Access to CCTV images

6.1 Access to recorded images will be restricted to certain authorised staff, and will not be made more widely available.

6.2 There must be sufficient security safeguards in place to prohibit interception and unauthorised access.

7. Subject Access Requests (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the GDPR

Staff must know how to respond to requests from individuals for access to CCTV recordings?

7.2 All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The school will respond to requests within **40 calendar days** of receiving the written request.

7.4 The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

8. Access to and Disclosure of Images to Third Parties

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the school where these would reasonably need access to the data (e.g. investigators).

8.2 Requests should be made in writing to the Headteacher (Police may arrive at school & view).

8.3 The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV within the school should be directed to the Headteacher in the first instance.

Further Information

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- General Data Protection Regulations (GDPR) 2018

Appendix 5 - CCTV Checklist

The CCTV system and the images produced are controlled by the Headteacher who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the GDPR Regulations 2018).

Enfield Learning Trust (ELT) has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of stakeholders. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (Date)	By	Date of Next Review
There is a named individual who is responsible for the operation of the system.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Staff and members of the school community will be consulted about the proposal to install CCTV equipment.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek			

advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			
The area is covered by CCTV surveillance, pictures are recorded and audio recording			

Appendix 6

Data Protection Impact Assessment (DPIA) (For use of surveillance CCTV in schools)

A. This is a Data Protection Impact Assessment (DPIA) statement for the use of surveillance CCTV at:

…….. (School Name)

…….. (School Address)

This assessment has been carried out by:

…….. (Name)

…….. (Position)

The assessment is effective from ….. / ….. / 20 … until review on ….. / ….. / 20 ….

The data controlling officer for the school is:

…….. (Name)

…….. (Position)

…….. (Telephone Contact)

…….. (Email Contact)

Registration with the Office of the Information Commissioner last updated on ….. / ….. / 20 ….

Checks for serviceability of CCTV systems and clarity of images last completed on
….. / ….. / 20 ….

B. Areas on the school covered by installed surveillance CCTV, whether active or not.
(At least this should include all outside areas on the school grounds, all entrances, all internal communal areas and all teaching units, individually stated where possible. Total number of possible operative cameras should be included.)

CAMERA AREA	No.		CAMERA AREA	No.

(A separate sheet should be completed for each area, giving precise details of the use of surveillance CCTV and the data collected from that area. It may be adequate to group together some areas where the information to be recorded is entirely or partially common, without loss of specific reference.)

C. Data Protection Impact Assessment (DPIA) for use of CCTV in …… (area)

Purpose(s) for use of surveillance CCTV:

Advantages of use of CCTV over other possible methods:

Assessment of amount of equipment used and time equipment is active:

Specific ways in which data collected will be used, including restrictions:

For stored data, the method used, the maximum length of time of storage, and how the data might be used:

All personnel having <u>immediate</u> access to data collected and stored, as part of specific duties:
(Included are any servicing company's personnel with general access).

Details of how data may be processed, by whom and what purpose(s):

Details of further personnel who may gain temporary access to data as part of their duties:

Methods of notification of the presence of surveillance CCTV and other information channels:

Details of all method(s) by which images, or collected data, from CCTV may be streamed to any outside agency or other parties, if relevant. Restrictions on access are also included:

Where an outside agency is entirely responsibly for the operation and control of the CCTV equipment, it's monitoring and the collection and use of data collected, all relevant and necessary details:

Assessment of any possible impact of CCTV surveillance on the right to privacy, performance or general well-being of any individuals:

Other relevant information: