The Blue Tangerine Federation

SPECIAL EDUCATIONAL NEEDS SCHOOLS

POLICIES, GUIDANCE AND PROCEDURES

Data Protection Policy and, Data Breach Response

Date Last Reviewed: September 2022
Staff Responsibility: Stephen Hoult-Allen
Date for Next Review: 1 September 2025

1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that The Collett school and St Luke's and their governors 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 The Schools are community and foundation schools and are the Data Controller for all the Personal Data processed by the Schools.

1.3 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.

1.4 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, governors, 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.

1.5 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 Schools to enforcement action by the Information Commissioner's Office (ICO), including the risk of fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the School's employees. At the very least, a breach of the GDPR could damage our reputation and have serious consequences for the Schools and for our stakeholders.

2. Status of the policy

1.1 This policy has been approved by the Governing Body of the Schools. 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 ensuring the School is compliant with the GDPR and with this policy. This post is held by Carole Connelly carole@schooldposervice.com and, Stephen Hoult-Allen, executivehead@bluetangerine.herts.sch.uk as our Deputy DPO.

3.2 The DPOs will play a major role in embedding essential aspects of the GDPR into the Schools' culture, from ensuring the data protection principles are respected to preserving data subject rights, recording data processing activities and ensuring the security of processing.

3.3 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:

3.3.1 senior management support;

3.3.2 time for DPOs to fulfil their duties;

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

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

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

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

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

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

3.4 The DPO is responsible for ensuring that the Schools' processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the schools must ensure the independence of the DPO.

3.5 The Schools 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 Governing Body.

3.6 The requirement that the DPO reports directly to the Governing Body ensures that the School's governors are made aware of the pertinent data protection issues. In the event that the Schools decide 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 Governing Body and to any other decision makers.

3.7 A DPO appointed internally by the Schools 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.

3.8 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, 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. As such, The Blue Tangerine Federation appoints the Schools' DPO Service and Carole Connelly as the school's DPO, with the Executive Headteacher as the Deputy DPO.

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

3.9.1 identify the positions incompatible with the function of DPO;

3.9.2 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;

3.9.3 include a more general explanation of conflicts of interests; and

3.9.4 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.

3.9.5 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 or Deputy DPO.

4. Definition of terms

4.1.1 **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;

4.1.2 **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;

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

4.1.4 **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.

4.1.5 **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.

4.1.6 **Data Users** include employees, volunteers, 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;

4.1.7 **Data Processors** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

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

4.1.9 **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;

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

4.1.11 **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;

4.1.12 **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.

5.2 Processed lawfully, fairly and in a transparent manner

5.2.1 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 Schools), 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.

5.2.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

5.2.2.1 where we have the Consent of the Data Subject;

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

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

5.2.2.4 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.

5.2.3 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.

5.3 Sensitive Personal Data

5.3.1 The School 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.

5.3.2 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 5.1 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

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

5.3.4 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;

5.3.5 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;

5.3.6 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.

5.3.7 The Schools recognise 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.

5.4 Biometric Data

5.4.1 The Schools may decide to 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.

5.4.2 Where Biometric Data relating to pupils is processed, the Schools must ensure that each parent of a child is notified of the schools' 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. The Schools must not process the Biometric Data if a pupil under 18 years of age where:

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

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

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

5.4.3 The Schools must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. The Schools will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.

5.4.4 The Schools must obtain the explicit Consent of staff, governors, or other Data Subjects before Processing their Biometric Data.

5.5 Criminal convictions and offences

5.5.1 There are separate safeguards in the GDPR for Personal Data relating to criminal convictions and offences.

5.5.2 It is likely that the Schools 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 and governors or due to information which we may acquire during the course of their employment or appointment.

5.5.3 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 Schools in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

5.5.4 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.

5.6 Transparency

5.6.1 One of the key requirements of the GDPR relates to transparency. This means that the Schools must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

5.6.2 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 School has developed privacy notices for the following categories of people:

5.6.2.1 Pupils

5.6.2.2 Parents

5.6.2.3 Staff and Volunteers

5.6.2.4 Governors

5.6.3 The Schools wish 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. 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 School premises or if we ask people to complete forms requiring them to provide their Personal Data.

5.6.4 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.

5.7 Consent

5.7.1 The Schools 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.

5.7.2 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.

5.7.3 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, the School should consider whether it is appropriate to inform Parents about this process. Consent is likely to be required if, for example, the School 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 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.[1]

5.7.4 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.

5.7.5 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.

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

6. Specified, explicit and legitimate purposes

6.1 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.

6.2 The Schools 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.

7. Adequate, relevant and limited to what is necessary

7.1 The Schools 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.

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

7.3 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 the schools function and we should not collect excessive data. We should ensure that any Personal Data collected is adequate and relevant for the intended purposes.

7.4 The Schools will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that the only members of staff or governors 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 Schools may adopt a layered approach in some circumstances, for example, members of staff or governors 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).

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

8. Accurate and, where necessary, kept up to date

8.1 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.

8.2 If a Data Subject informs the Schools of a change of circumstances their records will be updated as soon as is practicable.

8.3 Where a Data Subject challenges the accuracy of their data, the Schools 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 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.

8.4 Notwithstanding paragraph 8.3, 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 8.3 has been followed.

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

9.1 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.

9.2 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The Schools have a retention schedule for all data.

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

10.1 The Schools have 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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 Data Security 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.

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

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

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

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

10.7 It is the responsibility of all members of staff and 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 Executive Headteacher or the DPO.

10.8 Please see our Data Security Policy for details for the arrangements in place to keep Personal Data secure.

10.9 Governors

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

10.10.1.1 Ensure that Personal Data which comes into their possession as a result of their Schools duties is kept secure from third parties, including family members and friends

10.10.1.2 Ensure they are provided with a copy of the School's Data Security Policy.

10.10.1.3 Using a School email account for any School-related communications

10.10.1.4 Ensuring that any Schools-related communications or information stored or saved on an electronic device or computer is password protected and encrypted.

10.10.1.5 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.

10.10.2 Governors will be asked to read and sign an Acceptable Use Agreement.

11. Processing in line with Data Subjects' rights

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

11.1.1 withdraw Consent to Processing at any time;

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

11.1.3 request access to their Personal Data that we hold;

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

11.1.5 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;

11.1.6 restrict Processing in specific circumstances;

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

11.1.8 request a copy of an agreement under which Personal Data is transferred outside of the EEA;

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

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

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

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

11.1.13 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.

11.2 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.

12. Dealing with subject access requests

12.1 The GDPR extends to all Data Subjects a right of access to their own Personal Data. A formal request from a Data Subject for information that we hold about them must be made in writing. The School

can invite a Data Subject to complete a request form obtainable on line but we may not insist that they do so.

12.2 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 the Schools 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.

12.3 Any member of staff who receives a written request of this nature must immediately forward it to the Deputy DPO/ 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.

12.4 As the time for responding to a request does not stop during the periods when the Schools are 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.

12.5 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).

12.6 The Schools may ask the Data Subject for reasonable identification so that they can satisfy themselves about the person's identity before disclosing the information.

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

12.8 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 Schools, as Data Controllers, 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.

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

12.10 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 Schools consider the child to be mature enough to understand their rights under the GDPR, the Schools 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 Schools to disclose the Personal

Data to a Parent without the child's Consent). If Consent is not given to disclosure, the School shall not disclose the Personal Data if to do so would breach any of the data protection principles.[2]

12.11 It should be noted that the Education (Pupil Information) (England) Regulations 2005 (the "Regulations") applies to maintained schools so the rights available to parents in those Regulations to access their child's educational records apply to the Schools. This means that following receipt of a request from a parent for a copy of their child's educational records, the School must provide a copy within 15 school days, subject to any exemptions or court orders which may apply. The Schools may charge a fee for providing a copy of the educational record, depending on the number of pages as set out in the Regulations. This is a separate statutory right that parents of children who attend maintained schools have so such requests should not be treated as a subject access request.

12.12 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 School'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.

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

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

12.13.2 refuse to respond.

12.14 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.

12.15 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.

12.16 Further information about exemptions to be added as the Data Protection Bill is amended over time.

12.17 In the context of the Schools 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. 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 Schools 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.

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 School 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 Schools 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 Disclosure and Barring Service
14.2.4 the Teaching Regulation Agency
14.2.5 the Teachers' Pension Service
14.2.6 the Local Government Pension Scheme which is administered by HCC
14.2.7 our external HR provider
14.2.8 our external payroll provider
14.2.9 Our external IT Provider
14.2.10 HMRC
14.2.11 the Police or other law enforcement agencies
14.2.12 our legal advisors and other consultants
14.2.13 insurance providers
14.2.14 occupational health advisors
14.2.15 exam boards including
14.2.16 the Joint Council for Qualifications;
14.2.17 NHS health professionals including educational psychologists and school nurses;
14.2.18 Education Welfare Officers;
14.2.19 Courts, if ordered to do so;
14.2.20 Prevent teams in accordance with the Prevent Duty on schools;
14.2.21 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;
14.2.22 confidential waste collection companies;

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 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they

are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

14.5 All Data Sharing Agreements must be signed off by the Data Protection Officer who will keep a register of all Data Sharing Agreements.

14.6 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 requirements for contracts with Data Processors is set out in Appendix 1. It will be the responsibility of the Schools 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.

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

15.2 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.

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

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

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 As the Schools 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 – see Data Security Incident Response Plan further in this policy.

15.7 If a Security Incident Response Plan must be followed. In particular, the DPO or such other person identified in our Security Incident Response Plan must be notified immediately. You should preserve all evidence relating to the potential Personal Data Breach.

16. Accountability

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

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

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

16.2.2 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;

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

16.2.4 regularly training employees 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 School must maintain a record of training attendance by School 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 GDPR requires 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 School 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.

19. Privacy By Design and Data Protection Impact Assessment (DPIA)

19.1 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.

19.2 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:

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.

19.3.1 The School should conduct a DPIA and discuss the findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including:

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

19.3.1.2 Automated Processing including profiling and ADM;

19.3.1.3 large scale Processing of Sensitive Data; and

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

19.4 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.

19.5 A DPIA must include:

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

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

19.5.3 an assessment of the risk to individuals; and

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

20. Policy Review

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

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

21. Enquiries

21.1 Further information about the School's Data Protection Policy is available from school leaders, via the school office.

21.2 General information about the Act can be obtained from the Information Commissioner's Office: www.ico.gov.uk

Document Control

Date modified	Description of modification	Modified by
05.04.2018	Not relevant parts deleted e.g. CCT	Kasia Fejcher-Akhtar
16.08.2018	Refined corrections e.g. spellings and Data Retention Schedule added to the policy	Stephen Hoult-Allen
08.08.2019	Modified to reflect change in DPO	Manda Sides
10.01.2021	Changes to reflect information about DBS checks to be retained- Judicial review regarding the criminal record filtering rules - the supreme court ruling. Some convictions will now be spent and in addition there was a case in which a long serving member of staff was able to return from the office to the classroom as there was no "history" in the school of his previous conviction. The new rules came in end of November 2020.	Carole Connelly, Stephen Hoult-Allen
30.09.2022	No content changes except removal of the centre, FHEC.	Stephen Hoult-Allen

Data Breach Response Plan for The Collett School and St Luke's School

Introduction

1.2 Our schools have implemented appropriate technical and organisations measures to avoid data security breaches. However, in the event that a data security breach happens, we recognise that is important that the Schools are able to detect it and react swiftly and robustly in order to mitigate any risks to data subjects and to comply with our obligations under the General Data Protection Regulation ('GDPR').

1.3 This Data Breach Response Plan sets out how we will respond to any suspected or actual data breaches and should be read alongside our Data Protection Policy.

1.4 The procedures set out in this document are particularly important as, prior to the GDPR, there was no obligation on the Schools to notify the Information Commissioner's Office ('ICO') of data security breaches, although it was good practice to report serious breaches.

1.5 The GDPR requires the Schools to report 'notifiable breaches' without undue delay and, where feasible, not later than 72 hours after having become aware of it. Notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals. In the event that a report is not made within 72 hours, the Schools are required to provide the reasons for the delay in reporting it to the ICO.

1.6 If there is deemed to be a "high risk" to the rights and freedoms of individuals following a data breach, the School is also required to notify the individuals affected by the breach. However, in the interests of transparency, the Schools recognise that on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

1.7 If the School fails to report a notifiable personal data breach, we are at risk of receiving a sanction from the ICO, which may include a fine. Aside from our desire to avoid receiving any sanctions, the purpose of this Data Breach Response Plan is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

1.8 The Schools will ensure that staff are aware of and are trained on this Data Breach Response Plan to ensure it is effective should a data security incident occur. In particular, the [Data Response Team] identified below, must receive training on their roles and responsibilities should a breach occur. For example, our in-house IT team and our external IT support must be trained on how to identify if the security of our IT systems have been compromised and the steps that need to be taken to respond to a breach, for example, if data on a remote device needs to be wiped. Further details of our security procedures are set out in our Data Protection Policy.

1.9 We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this Data Breach Response Plan to ensure that we can react promptly in the event that a breach or suspected breach occurs. Any member of staff who becomes aware of a suspected or actual personal data breach must follow the escalation procedures set out below. Failure to comply with these procedures may be a disciplinary issue.

1.2 The Schools' DPO is Carole Conelly, the Deputy DPO is Stephen Hoult-Allen

2 What is a personal data breach?

2.1 The legal definition of a personal data breach is, "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."

2.2 A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

2.2.1 Loss or theft of data or equipment;

2.2.2 People gaining inappropriate access to personal data;

2.2.3 A deliberate attack on systems;

2.2.4 Equipment failure;

2.2.5 Human error;

2.2.6 Acts of God (for example, fire or flood);

2.2.7 Malicious acts such as hacking, viruses or deception.

2.3 Breaches can be categorised according to the following three well-known information security principles:

2.3.1 "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data;

2.3.2 "Integrity breach" - where there is an unauthorised or accidental alteration of personal data;

2.3.3 "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

2.4 Depending on the circumstances, a breach can relate to the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

2.5 A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

2.6 A security incident resulting in personal data being made unavailable for temporary period is also a type of breach, as the lack of access to the data could have a significant impact on the rights and freedoms of data subjects, for example, if our IT system goes down. This type of breach should be recorded in the Schools' Data Breach Log set out in Appendix 1 so that we keep records of all such incidents. However, depending on the circumstances of the breach, it may or may not require notification to the ICO and communication to affected individuals.

2.7 Where personal data is unavailable due to planned system maintenance being carried out, this should not be regarded as a 'breach of security'.

3 Understanding the risk to the rights and freedoms of individuals

3.1 A breach can potentially have a number of consequences for individuals, which can result in physical, material, or non-material damage. This can include loss of control over their personal data, limitation

of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

3.2 When assessing the risk to individuals, the DPO must consider the following factors:

3.2.1 the type of breach;

3.2.2 the nature, sensitivity, and volume of personal data;

3.2.3 ease of identification of individuals;

3.2.4 severity of consequences for individuals;

3.2.5 special characteristics of the individual;

3.2.6 special characteristics of the data controller; and

3.2.7 the number of affected individuals.

4 Timescales for reporting a breach

4.1 The Schools are required to report a notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

4.2 It is likely that the Schools will be deemed as having become "aware" of a breach when we have a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised. The GDPR expects us to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place. This puts an obligation on us to ensure that we will be "aware" of any breaches in a timely manner so that we can take appropriate action.

4.3 While some breaches may be obvious, in other cases we may need to establish whether personal data has been compromised. In such circumstances, we will investigate promptly in accordance with the procedures below to determine whether a breach has happened which, in turn, will enable us to decide if remedial action is needed and if the breach needs to be notified to the ICO and the affected data subjects.

4.4 It is possible that we may not have established all of the relevant facts following a data security breach or completed our investigation within 72 hours. However, in the event that the School determines that a breach has taken place and that it needs to be notified to the ICO, a report should be made within 72 hours with the information held at that point in time. In these circumstances, the report to the ICO should explain that further information will be provided as and when it is available.

4.5 It is possible that some breaches may come to the attention of a member of staff or may be flagged up by our IT systems. However, it is also possible that we may be notified about breaches by third parties, such as the people who are affected by the breach, a data processor or by the media.

4.6 In the event that we investigate a suspected breach and we are able to establish that no actual breach has occurred, the Data Breach Log in Appendix 1 must still be completed so that we can keep records

of ‘near misses’ or other weaknesses in our systems and procedures in order to continuously review and improve our processes.

5 Response plan[3]

5.1 A member of staff within a school who becomes aware of a suspected or actual data security breach must inform the Head of School OR the Executive Headteacher OR the DPO of the School OR the Deputy DPO of the school by email without delay[4]. The Executive Headteacher should be copied in to the email to the DPO[5].

5.2 A member of staff who becomes aware of a suspected or actual data security breach must inform the DPO or Deputy DPO by email without delay[6]

5.3 If a member of staff is unsure if a breach has happened, the above procedures must still be followed without delay so that the suspected breach can be investigated in order to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the data subjects.

5.4 The Deputy DPO will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the DPO. If not decided not to escalate it to the DPO, the Data Breach Log in Appendix 1 must be completed as accurately as possible, including the reasons why the incident does not need to be escalated to the DPO. The Data Breach Log should be emailed to the DPO without delay for record keeping purposes][7].

5.5 If the Deputy DPO decides to escalate a breach or suspected breach to the DPO, they must do so without delay. Where possible, the Data Breach Log in Appendix 1 must be completed with as much information as possible and emailed to the DPO. However, if it is not convenient or practicable to complete the Data Breach Log, the report can be made by setting the information out in an email.[8]

5.6 Once a breach or suspected breach has been reported to the DPO, the DPO must commence an investigation and assess whether he / she has sufficient information to identify next steps. The purpose of the investigation is to:

5.6.1 establish if a breach has happened;

5.6.2 establish the nature and cause of the breach;

5.6.3 establish the extent of the damage or harm that results or could result from the breach;

5.6.4 identify the action required to stop the data security breach from continuing or recurring; and

5.6.5 mitigate any risk of harm that may continue to result from the breach.

5.7 The DPO should contact the Executive Head/ head of school/member of staff who made the report[9] if further information is required. The DPO may also need to speak to the member of staff who first reported the breach or suspected breach.

5.8 During the course of his or her investigation, the DPO should consider whether to involve the Deputy DPO.

5.9 If the DPO is unavailable for any reason, for example, the DPO is on annual leave, on sickness absence or is otherwise not available to respond to the data breach, then the Deputy DPO must fulfil the responsibilities of the DPO set out in this Data Breach Response Plan. The Deputy DPO must have access to the email account identified above to which data breaches are reported.

5.10 The DPO should consider whether input is required from the Schools' IT or HR support in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach. The Schools have external HR IT support.

5.11 Depending on the circumstances, the DPO should also consider whether the Schools' insurers should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police and the Local Authority. The DPO should also consider if specialist IT support is required in order to contain and manage a breach and whether the Schools' Communications should be engaged if it is likely that we will need to communicate internally and / or externally with our stakeholders regarding the breach or suspected breach.

5.12 If the breach or suspected breach has occurred at one of our Data Processors, the DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to data subjects. It remains the Schools' responsibility to decide whether to report any such breach to the ICO within 72 hours.

5.13 The same requirement applies if the breach or suspected breach is reported to us by a joint Data Controller though in this case we need to establish with the joint Data Controller who is going to report the breach to the ICO and the data subjects if such notification is required.

5.14 Depending on the timescales as to when a member of staff originally became aware of a breach, the DPO must be mindful of the requirement to notify the ICO without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. As stated above, it is therefore possible that a data security breach may need to be reported to the ICO before the Schools have fully investigated or contained the breach. A report to the ICO must contain the following information:

5.14.1 the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned;

5.14.2 the name and contact details of the DPO or other contact point where more information can be obtained;

5.14.3 the likely consequences of the personal data breach;

5.14.4 the measures taken or proposed to be taken by the Schools to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects[10].

5.15 The DPO is not required to provide precise details in the report to the ICO if this information is not available and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The DPO should inform the ICO

if the Schools do not yet have all the required information and if further details will be provided later on.

5.16 If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

5.17 In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay with the reasons for the delay.

5.18 If the DPO concludes that a referral to the ICO is required and also concludes that there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach then the data subjects affected by the breach must also be notified without undue delay. The DPO must liaise with the [Executive Head [and] [Chief Executive Officer] in relation to how the issue should be communicated to the relevant stakeholders. The DPO will need to consider which is the most appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information:

5.18.1 description of the nature of the breach;

5.18.2 the name and contact details of the DPO or other contact point;

5.18.3 a description of the likely consequences of the breach; and

5.18.4 a description of the measures taken or proposed to be taken by the Schools to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

[Given that a large number of our stakeholders are children, if a data breach affects our pupils, it is likely that the above information will need to be given to parents / carers if the affected pupils are aged 12 or under. If the affected pupils are aged 13 or over, the pupils should be informed and it may also be appropriate to notify parents / carers, depending on the circumstances and the nature of the personal data which has been compromised.

5.19 If the DPO decides to notify data subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included. The Schools should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

5.20 The DPO must complete the Data Breach Log before making the referral to the ICO and keep it under review as and when further information comes to light.

5.21 In certain circumstances, where justified, and on the advice of law-enforcement authorities, the Schools may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

5.22 Even if the DPO initially decides not to communicate the breach to the affected data subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

5.23 In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the DPO must still complete the Data Breach Log in Appendix 1 and clearly set out the reasons why the DPO is satisfied that a referral is not required. The DPO must keep the decision under review and be prepared to make a referral to the ICO if any circumstances change or if any information comes to light which means that a referral should be made.

5.24 Once the breach has been contained and action taken to stop or mitigate the breach, the DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

5.25 As part of the review process, the DPO should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the Schools' response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any amendments need to be made to it.

5.26 Where security is found not to be appropriate, the DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

5.27 Where a data processor caused the breach, the DPO should consider whether adequate contractual obligations were in place to comply with the GDPR and if so, whether the data processor is in breach of contract.

6 School holidays

6.1 The Schools recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the schools are closed/ have limited staff available during school holidays. A breach may still occur during these periods and we will implement the following steps to mitigate any risk caused if a breach happens during the school holidays:

6.1.1 The DPO and a Deputy DPO's email address will be made available to staff and will be available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

6.1.2 The DPO and Deputy DPO will have the contact details for the Executive Headteacher - our IT support and our legal advisors and our insurers so that action can be taken without delay should a breach occur.

6.1.3 The DPO and Deputy DPO should follow the steps set out above as best as he / she can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the school has limited staff available due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the Schools should take to mitigate any risks.

7 Review

7.1 This Data Breach Response Plan will be kept under review by the DPO and may be revised to reflect good practice or changes to our organisational structure.

Data Breach Log for The Collett School and St Luke's School

This Data Breach Log must be completed by a suitably trained person following any reports of a security breach or suspected breach involving personal data. Staff must follow the Schools' Data Breach Response Plan following notification of a breach or suspected breach. In the event you are unsure whether to notify the ICO and the data subjects, you should obtain legal advice without delay as the ICO must be informed about notifiable breaches within 72 hrs.

Information	Response
Date and time this record was completed	
Name of person completing this record	
General description of the breach	
Name and job title of person who originally reported the breach / suspected breach	
Date and time the breach / suspected breach was reported	
Who was the breach / suspected breach reported to?	
Has the Data Protection Officer been informed?	
Has the Data Breach Response Team been notified?	
What are the details of the breach / suspected breach (include as much detail as possible) NB: An investigation must be undertaken where appropriate	

Information	Response
Who is responsible for the breach i.e. the school as data controller, a joint data controller or a data processor?	
Is the breach ongoing or has it been contained?	
Is any other information required in order to assess the extent of the breach / the risk to data subjects? If so, specify that information here.	
Whose data has / may have been compromised as a result of the breach / suspected breach?	
Type of data involved in the breach / suspected breach	
Does the breach / potential breach involve sensitive personal data[11] or information about criminal offences?	
What is the likely risk to individuals?	
Is there likely to be a high risk to individuals?	
Does the breach need to be reported to the ICO? If yes, and if the breach happened more than 72 hours ago, what is the reason for the delay if notifying the ICO?	
If the breach has already been reported to the ICO, confirm the date and time the report was made, who made the report and whether the report was made within 72 hours	

Information	Response
If a report has been made to the ICO, what advice or recommended actions have been given? Specify any sanctions that are issued by the ICO following a breach.	
If a report to the ICO is not being made, confirm the reasons why and whether the decision needs to be kept under review	
Do the data subjects affected need to be notified about the breach? If so, confirm who will notify them and how and when they will be notified. If data subjects are not going to be informed, explain the reasons why.	
Does the breach need to be reported to the Police?	
Do any other steps need to be taken e.g. comms to stakeholders, provision of complaints policy, consult legal advisors, notify insurers, external IT support.	
Is there likely to be press / media interest as a result of the breach? If so, have the appropriate protocols for handling media enquires been followed?	
Outline the actions that need to be taken in response to the breach / suspected breach to reduce the risk of a re-occurrence and who is responsible for implementing them and the relevant timescales. This should include whether an	

Information	Response
investigation under the school's disciplinary policy is recommended. NB: The information provided in response to this question is likely to be a summary as a more detailed report / audit is likely to be required following a data breach which is notified to the ICO.	

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))

Appendix 2: Managing our data sources

Responsibilities

The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the DPO or Deputy DPO. The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

Managing Pupil Records

The pupil record should be seen as the core record charting an individual pupil's progress through the Education System. The pupil record should accompany the pupil to every school they attend and should contain information that is accurate, objective and easy to access. These guidelines are based on the assumption that the pupil record is a principal record and that all information relating to the pupil will be found in the file (although it may spread across more than one file cover).

Items which should be included on the pupil record

- If the pupil has attended an early years
- Admission details
- Privacy Notice [if these are issued annually only the most recent need be on the file]
- Photography Consents
- Annual Written Report to Parents
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- EHCP and related plans
- Any relevant medical information
- Child protection reports/disclosures (should be stored in the file in a sealed envelope clearly marked as such)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil

Other information:

- Absence notes
- Parental consent forms for trips/outings [in the event of a major incident all the parental consent forms should be retained with the incident report not in the pupil record]
- Correspondence with parents about minor issues
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy could be placed on the pupil file in the event of a major incident)

Transferring the pupil record to college

The pupil record should not be weeded before transfer to the secondary school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage.

Files should not be sent by post unless absolutely necessary. If files are sent by post, they should be sent by registered post with an accompanying list of the files. The secondary school should sign a copy of the list to say that they have received the files and return that to the primary school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes.
Electronic documents that relate to the pupil file also need to be transferred, or, if duplicated in a master paper file, destroyed.

E-mail
As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that e-mail should be laid out and formulated to your school's standards for written communications.

E-mail is not always a secure medium to send confidential information
You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a civil penalty of up to £500,000 from the Information Commissioner or it could end up on the front page of a newspaper. Confidential orsensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

E-mail is disclosable under the access to information regimes
All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately
E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.

E-mail can form a contractual obligation
Agreements entered into by e-mail can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else
All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.
Employers must be careful how they monitor e-mail
Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring.

E-mail is one of the most common causes of stress in the work-place
Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent thishappening.

Creating and sending e-mail

- Do I need to send this e-mail?
- Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.
- To whom do I need to send this e-mail?
- Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary.
- Never send on chain e-mails.
- When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.
- Use a consistent method of defining a subject line
- Having a clearly defined subject line helps the recipient to sort the e-mail on receipt.
- A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

- Do not use text language or informal language in schoole-mails.
- Always sign off with a name (and contact details).
- Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
- Never write an e-mail in capital letters. This can be interpreted as shouting.
- Always spell check an e-mail before you send it.
- Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
- If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep thee-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school. There is some debate about how enforceable disclaimers are. Legal advice should be sought when using or drafting a disclaimer for your organisation to ensure it meets your specific needs.

Managing received e-mails

- Manage interruptions
- Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.
- Turn off any alert that informs you e-mail has been received.
- Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

Use rules and alerts

- By using rules and alerts members of staff can manage their inbox into theme-based folders. For

example:

- E-mails relating to a specific subject or project can be diverted to a named project folder
- E-mails from individuals can be diverted to a specificfolder

Warn senders that you will assume that if you are copied in to an e-mail, the message is for information only and requires no response from you.

Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example:"For Action:", FYI:",etc)

Use electronic calendars to invite people to meetings rather than sending e-mails asking them to attend

Using an out of office message

If you check your e-mail at stated periods during the day you can use an automated response to incoming e-mail which tells the recipient when they might expect a reply. A sample message might read as follows: Thank you for your e-mail. I will be checking my e-mail at three times today, 8:30am, 1:30pm and 3:30pm. If you require an immediate response to your e-mail please telephone me on xxxxxxxxx. This gives the sender the option to contact you by phone if they need an immediate response.

Filing e-mail

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

E-mail text and attachments

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information which makes up the audit trail, is to save the e-mail in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS Outlook, or by using the"save as" function to save the e-mail in an electronic filing system. If the e-mail needs to be re-sent it will automatically open into MS Outlook.

Where appropriate the e-mail and the attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the e-mail in .msg format will.

E-mail text only

- If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes.
- Alternatively the e-mail can be saved in .html or .txt format. This will save all the text in the e-mail and a limited amount of the audit information. The e-mail cannot be re-sent if it is saved in this format.
- The technical details about how to undertake all of these functions are available in application Help functions.

How long to keep e-mails?

- E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards.
- Aim to delete emails every three to six months.
- E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond

with the classes of records according to content in the retention schedule for schools . These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

Unauthorised access, theft or loss

- Staff should be encouraged not to take personal data on staff or students out of the school unless there is no other alternative. Records held within the school should be in lockable cabinets.
- Consider restricting access to offices in which personal information is being worked on or stored. All archive or records storage areas should be lockable and have restricted access.
- Where paper files are checked out from a central system, log the location of the file and the borrower, creating an audit trail.
- For the best ways of disposing of sensitive, personal information see Safe Disposal.

Clear Desk Policy

A clear desk policy is the best way to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/ or flood damage.

A clear desk policy involves the removal of the physical records which contain sensitive personal information to a cupboard or drawer (lockable where appropriate). It does not mean that the desk has to be cleared of all its contents.

Disclosure

Staff should be made aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it. Ensure that where you intend to share personal information with a third party that you have considered the requirements of the Data Protection Act. Be careful of giving out personal information over the telephone; invite the caller to put the request in writing, supplying a return address, which can be verified.

Transferring information – HfL LARA (Login Anywhere Remote Access)

All staff are able to connect to a full desktop hosted within their school network. It will give users access to all their normal in school-mapped drives, along with most school specific software. E.g. SIMS, FMS etc. This is the most secure way to access files outside of the school as it prevents users from saving files back to their laptop/PC. We do not use Data Pens/FlashDrives etc.

Responding to Incidents

In the event of an incident involving the loss of information or records the school should be ready to pull together an incident response team to manage the situation. Stephen Hoult-Allen should be contacted to deal with any press issues.

Major Data Loss/Information Security Breach

- If there is a major data loss or information security breach the DPO, Deputy DPO and Executive Headteacher must be informed immediately.
- Do not put off informing the Information Commissioner's Office if the incident is serious enough to justify notification. It is better to have notified the Information Commissioner before someone makes a complaint to him.

School Closures and Record Keeping

When a school closes records management is the responsibility of each Local Authority [LA] to manage the records of closed schools until they have reached the end of their administrative life and to arrange for their disposal when required.

Disposal of records that have reached the end of the minimum retention period allocated

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip.

Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed

Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove that the electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

Digital Continuity

The long term preservation of digital records is more complex than the retention of physical records. A large number of organisations create data in electronic format which needs to be retained for longer than 7 years. If this data is not retained in accessible formats the organisation will be unable to defend any legal challenge which may arise.

In order to ensure that digital records are retained in a way that ensures they can be retrieved in an accessible format when they are required, all records which are required to be retained for longer than 6 years should be part of a digital continuity statement.

The average life of a computer system can be as little as 5 years, however, as digital continuity is resource intensive, only records which are required to be retained for 6 years (in line with the Limitation Act 1980) or longer should be subject to digital continuity statements.

Storage of records

- Where possible records subject to a digital continuity statement should be "archived" to dedicated server space which is being backed up regularly.
- Where this is not possible the records should be transferred to high quality CD/DVD, if they are to be included with paper documentation in a paper file or onto an external hard drive which is clearly marked and stored appropriately. Records stored on these forms of storage media must be checked regularly for data degradation.
- Flash drives (also known as memory sticks) must not be used to store any records which are subject to a digital continuity statement. This storage media is prone to corruption and can be easily lost or stolen.
- Storage methods should be reviewed on a regular basis to ensure that new technology and storage methods are assessed and where appropriate added to the digital continuity policy.

Migration of Electronic Data

Migration of electronic data must be considered where the data contained within the system is likely to be required for longer than the life of the system. Where possible system specifications should state the accepted file formats for the storage of records within the system.

If data migration facilities are not included as part of the specification, then the system may have to be retained in its entirety for the whole retention period of the records it contains. This is not ideal as it may mean that members of staff have to look on a number of different systems to collate information on an individual or project. Software formats should be reviewed on an annual basis to ensure usability and to avoid obsolescence.

Degradation of Electronic Documents

In the same way as physical records can degrade if held in the wrong environmental conditions, electronic records can degrade or become corrupted. Whilst it is relatively easy to spot if physical records are becoming unusable it is harder to identify whether an electronic record has become corrupted, or if the storage medium is becoming unstable.

When electronic records are transferred from the main system to an external storage device, the data should be backed up and two safe copies of the data should be made. The data on the original device and the back-ups should be checked periodically to ensure that it is still accessible. Additional back-ups of the data should be made at least once a year and more frequently if appropriate.

Where possible digital records should be archived within a current system, for example, a designated server where "archived" material is stored or designated storage areas within collaborative working tools such as SharePoint.

Internationally Recognised File Formats

Records which are the subject of a digital continuity statement must be "archived" in one of the internationally recognised file formats.

Digital Continuity Strategy Statement

Statement of business purpose and statutory requirements for keeping records

The Collett School and St Luke's School are education schools for pupils with complex needs. We are bound by the legislation to keep children safe, whilst also abiding by the requirements of GDPR. We have a retention schedule within our Data Protection policy.

Names of the people/functions responsible for long term data preservation
The Executive Headteacher, Stephen Hoult-Allen holds responsibility for long term data preservation and the post holder responsible for the information assets.

If the responsibility is not clearly assigned there is the danger that it may disappear as part of a restructure process rather than be reassigned to a different post.

Description of when the record needs to be captured into the approved file formats
The record may not need to be captured in to the approved file format at its creation. For example, an MSWord document need not be converted to portable document format until it becomes semi-current. The digital preservation statement should identify when the electronic record needs to be converted to the long term supported file formatsidentified above.

Description of the appropriate supported file formats for long term preservation
This is agreed, when required with the appropriate technical staff.

Retention of all software specification information and licence information
Held with SITTS

Description of where the information asset is to be stored.
With SITTS

Description of how access to the information asset is to be managed within the data security protocols
The data held for long term preservation must be accessible when required but also must be protected against the standard information security requirements which are laid down for records within the authority. Accessing the records and the information is through a tiered level of permissions with individuals having access only through password protection.

Appropriate Storage for Physical Records
Records must be stored in the workplace in a way that does not cause a health and safety hazard. Records must not be stored in corridors or gangways and must not impede or block fire exits. There should be where appropriate, heat/smoke detectors connected to fire alarms, a sprinkler system and the required number of fire extinguishers. The area should be secured.

Storage areas should be regularly monitored and checked for any damage or emerging risks, especially during holiday periods.

The following are hazards are considered before approving areas where physical records can be stored.

Environmental Damage - Fire
Records can be damaged beyond repair by fire. Smoke and water damage will also occur to records which have been in a fire, although generally records damaged by smoke or water can be repaired. Core records are kept in cabinets or cupboards. Metal filing cabinets within locked rooms are used.

Environmental Damage - Water
Records damaged by water can usually be repaired by a specialist document salvage company. The salvage process is expensive, therefore, records need to be protected against water damage where possible. Where flooding is involved the water may not always be clean and records could become contaminated as well as damaged.

Records should not be stored directly under water pipes or in places that are liable to flooding (either from excess rainfall or from the overflow of toilet cisterns). Records should be stored in cabinets/cupboards with tight fitting doors which provide protection from water ingress. Records stored on desks or in cabinets/cupboards without close fitting doors will suffer serious water damage.

Records should be stored at least 2 inches off the ground. Most office furniture stands 2 inches off the ground. Portable storage containers (i.e. boxes or individual filing drawers) should be raised off the ground by at least 2 inches. This is to ensure that in the case of a flood that records are protected against immediate flood damage.

Storage areas should be checked for possible damage after extreme weather to ensure no water ingress has occurred.

Environmental Damage – Sunlight
Records should not be stored in direct sunlight (e.g. in front of a window). Direct sunlight will cause records to fade and the direct heat causes paper to dry out and become brittle.

Environmental Damage – High Levels of Humidity
Records should not be stored in areas which are subject to high levels of humidity. Excess moisture in the air can result in mould forming on the records. Mould can be a hazard to human health and will damage records often beyond repair.

Temperature and humidity should be regularly monitored. Storage areas should be checked for damage after extreme weather conditions to reduce the risk of mould growth.

Environmental Damage – Insect/Rodent Infestation
Records should not be stored in areas which are subject to insect infestation or which have a rodent problem (rats or mice).