The Leys Primary & Nursery School

Data Protection Policy

(Including Retention Periods)

Approved by:	Resources Committee	**Date:**	23/02/22
Next review due by: Resources Committee	Feb 2025		

1. Policy statement and objectives

1.1 The objectives of this Data Protection Policy are to ensure that The Leys Primary & Nursery School and its 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 school is a community school and is the Data Controller for all the Personal Data processed by the school.

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 school 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 school and for our stakeholders.

2. Status of the policy

1.1 This policy has been approved by the Governing Body of the School. 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[1]

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 Patrick Aikman, patrick@schoolDPOservice.com. Any questions or concerns about the operation of this policy should be referred in the first instance to the DPO.

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

3.3 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:

[1] This section assumes that the DPO will be an internal appointment. It will need to be amended if the DPO is an external appointment.

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 School's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the school must ensure the independence of the DPO.

3.5 The school 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 school decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the Governing Body and to any other decision makers.

3.7 A DPO appointed internally by the school 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.

3.9 In the light of this and in the event that the school decides to appoint an internal DPO, the School 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.

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

4. Definition of terms

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

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

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

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

4.5 **Data Controllers** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

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

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

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

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

4.10 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

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

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

4.13 **Sensitive Personal Data** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5. Data protection principles

5.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

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

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

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

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

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

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

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 school), 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:

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

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

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

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

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

5.4 Criminal convictions and offences

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

5.4.2 It is likely that the school 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.

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

5.4.4 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.

5.5 Transparency

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

5.5.2 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:

5.5.2.1 Parents

5.5.2.2 Staff

5.5.2.3 Governors & Volunteers

5.5.3 The school wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. 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.

5.5.4 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.

5.6 Consent

5.6.1 The school 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.

5.6.2 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.

5.6.3 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). 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 is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent if the pupil is aged under 13.

5.6.4 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.

5.6.5 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.

5.6.6 Evidence and records of Consent must be maintained so that the school 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 school 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 school 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 school 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 the all the information is required. We may only collect Personal Data that is needed to operate as a school 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 school 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 School 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 school's 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 school 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 school 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 school has a retention schedule for all data as set out in appendix 2.

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

10.1 The school has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

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 Program 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 Headteacher or the DPO.

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

10.9 Governors

10.9.1 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 school's data protection processes as part of their induction and should be informed about their responsibilities to keep Personal Data secure. This includes:

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

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

10.9.1.3 Using a school email account for any School-related communications.

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

10.9.1.5 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.

10.9.2 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 form, 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 school 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 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 School is closed for the holidays, we will attempt to mitigate any impact this may have on the rights of data subjects to request access to their data by implementing the following measures: - Our DPO will be available during the period when the school is shut and if necessary key staff can be available during holiday periods.

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 school 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 school, as Data Controller, to assess whether the child is capable of understanding their rights under the GDPR and the implications of their actions, and so decide whether the Parent needs to make the request on the child's behalf. A Parent would normally be expected to make a request on a child's behalf if the child is younger than 13 years of age.

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).

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 school. 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 school 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 school 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 once the Data Protection Bill becomes law.

12.17 In the context of a School 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 school whilst also applying common sense to the particular circumstances. In particular they should:

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

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

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

14. Authorised disclosures

14.1 The 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 school 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 Herts For Learning our HR provider

14.2.8 SERCO - our external payroll provider

14.2.9 Our external IT Provider & Herts for Learning IT Support

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 our insurance providers – HCC

14.2.14 our staff absence insurers – Schools Advisory Service

14.2.15 occupational health advisors

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 school 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 school. 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 School is closed or has 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. During school holidays the admin e-mail will be monitored once a week and any information regarding a personal data breach will be forwarded to our DPO who monitor their emails daily including throughout school holidays.

15.7 If a member of staff or governor knows or suspects that a Personal Data Breach has occurred, our DPO the DPO must informed without delay.

16. Accountability

16.1 The school must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The school is 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. CCTV

21. The school uses CCTV in locations around the school site. This is to:

21.1.1 protect the school buildings and their assets.

21.1.2 increase personal safety and reduce the fear of crime.

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

21.1.4 assist in identifying, apprehending and prosecuting offenders.

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

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

21.1.7 assist in managing the school.

21.2 Please refer to the School's CCTV policy for more information[2].

22. Policy Review

22.1 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.

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

23. Enquiries

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

[2]The School must ensure that it has a more comprehensive CCTV policy which is compliant with the ICO's Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

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

Document Control[3]

Date modified	Description of modification	Modified by

[3]This policy should be reviewed by the school periodically and at least every 2 years. It is important to ensure that the DPO is aware of his or her obligations under this policy and that they receive the training and other support they need in order to fulfil this role.

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 – Retention – School Management

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL[1]
1.1.2	Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
	Inspection Copies[2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they must be shredded.
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports, then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4	Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL

1 In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a crosscut shredder.

2 These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

1.1 Governing Body (continued)

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.5	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9	Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11	Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL

Please note that all information about the retention of records concerning the recruitment of Head Teachers can be found in the Human Resources section below.

1.2 Head Teacher and Senior Management Team

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Logbooks of activity in the school maintained by the Head Teacher	There may be data protection issues if the logbook refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refer to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		Date of correspondence + 3 years then SECURE DISPOSAL review	SECURE DISPOSAL
1.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7	School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.1	All records relation to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.[3]	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
1.3.5	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
1.3.6	Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Current year + 1 year	SECURE DISPOSAL

3 School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014 p6

1.3 Admissions Process (continued)

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.7	Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
	For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL

1.4 Operational Admissions

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2	Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3	Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4	Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL

2. Human Resources

This section deals with all matters of Human Resources management within the school.

2.1 Recruitment

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.1.1	All records leading up to the appointment of a new Headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2	All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL
2.1.3	All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked, and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation, then this should be placed on the member of staff's personal file	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

4 Employers are required to take a "clear copy" of the documents which they are shown as part of this process

2.2 Operational Staff Management

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.3.1	Allegation of a child protection nature against a member of staff including where the allegation is unfounded[5]	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found, they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning[6] + 6 months	SECURE DISPOSAL [If warnings are placed on personal files, then they must be weeded from the file]
	written warning – level 1			Date of warning + 6 months	
	written warning – level 2			Date of warning + 12 months	
	final warning			Date of warning + 18 months	
	case not found			If the incident is child protection related, then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

5 This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention

6 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice

2.4 Health and Safety

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.4.1	Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2	Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents, a further retention period will need to be applied	SECURE DISPOSAL
2.4.4	Accident Reporting	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		SECURE DISPOSAL
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8	Fire Precautions logbooks	No		Current year + 6 years	SECURE DISPOSAL

3. Financial Management of the School

This section deals with all aspects of the financial management of the school including the administration of school meals.

3.1 Risk Management and Insurance

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL

3.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4	All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
3.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management

This section covers the management of buildings and property.

4.1 Property Management

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.1.1	Title deeds of properties belonging to the school	No		PERMANENT These should follow the property unless the property has been registered with the Land Registry	
4.1.2	Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
4.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance logbooks	No		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety above.

5.1 Pupil's Educational Record

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
	Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: ● to another primary school ● to a secondary school ● to a pupil referral unit ● If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
	Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Pupil Copies	Yes			
	Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.

	Internal			This information should be added to the pupil file	

5.1 Pupil's Educational Record (continued)

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention					
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.

5.2 Attendance

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability	Date of birth of the pupil + 25 years [This would normally be retained on	SECURE DISPOSAL unless the document is subject to a legal hold

			Act 2001 Section 14	the pupil file]	

6. Curriculum Management

6.1 Statistics and Management Information

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2	Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
	SATS records –	Yes			
	Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL

6.2 Implementation of Curriculum

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.2.1	Schemes of Work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.2	Timetable	No		Current year + 1 year	
6.2.3	Class Record Books	No		Current year + 1 year	
6.2.4	Mark Books	No		Current year + 1 year	
6.2.5	Record of homework set	No		Current year + 1 year	
6.2.6	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL

Extra-Curricular Activities

7.1 Educational Visits outside the Classroom

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time.
7.1.4	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	

7.2 Walking Bus

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.2.1	Walking Bus Registers	Yes		Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]

7.3 Family Liaison Officers and Home School Liaison Assistants

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
7.3.1	Day Books	Yes		Current year + 2 years then review	
7.3.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3	Referral forms	Yes			While the referral is current
7.3.4	Contact data sheets	Yes			Current year then review, if contact is no longer active then destroy
7.3.5	Contact database entries	Yes			Current year then review, if contact is no longer active then destroy
7.3.6	Group Registers	Yes			Current year + 2 years

8. Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority.

8.1 Local Authority

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1	Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4	Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL

8.2 Central Government

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.2.1	OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2	Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3	Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL