DATA PROTECTION POLICY

Last review date	September 2019
Date approved by the Trust Board	
Date for next review	September 2020

Table of Contents

Introduction

The Leading Edge Academies Partnership (the 'Trust') is a team of school leaders that aim to be Leading Edge and pioneering in their approach to education and well-being. We are a growing family of like-minded schools that offer a values based education to the communities we serve and welcome staff, workers, students, parents/carers and volunteers from all different ethnic groups and backgrounds.

The term 'Trust Community' includes all staff, trustees, governors, students, parents/carers, volunteers and visitors.

We are a values based Trust, which means all actions are guided by our six 'Es' as follows:

- **Ethical** – 'Doing the right thing'
- **Excellence** – 'Outstanding quality'
- **Equity** – 'Fairness and social justice'
- **Empathy** – 'Caring for others'
- **Evolution** – 'Continuous change'
- **Endurance** – 'Working hard and not giving up'

This policy is based on the value of being **'Ethical'**

1. Aims

The Leading Edge Academies Partnership aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Leading Edge Academies Partnership processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller.

The Leading Edge Academies Partnership is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our academy, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that the Leading Edge Academies Partnership complies with all relevant data protection obligations.

5.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, report to the board their advice and recommendations on the Leading Edge Academies Partnership data protection issues.

The Data Manager is also the first point of contact for individuals whose data the academy processes. The DPO is responsible for overseeing the work of Data Managers in every Leading Edge Academies Partnership school and recording data breaches and reporting where appropriate to the ICO.
Full details of the DPO's responsibilities are set out in their job description.
Our DPO is Mr Andrew Harvey and is contactable via phone on 01736 363240

5.3 Principals
The Principal act as the representative of the data manager on a day-to-day basis.

5.4 All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the academy of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our academy must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Leading Edge Academies Partnership aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the academy can **fulfil a contract** with the individual, or the individual has asked the academy to take specific steps before entering into a contract
- The data needs to be processed so that the academy can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the academy, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the academy or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).
Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the academy's Information and Records Management Society's toolkit for schools

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and Boards of Trustees where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests
Individuals have a right to make a 'subject access request' to gain access to personal information that the Leading Edge Academies Partnership holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our academies may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.
A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

As an academy trust, parents, or those with parental responsibility do not have an automatic parental right of access to their child's educational record. However, it is the Leading Edge Academies Trust's policy to allow parental access to their child's data on receipt of a written request.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The academy will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use *the Leading Edge Academies Trust's* biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash using our revaluation unit and accessing it with a PIN.

Parents/carers and pupils can object to participation in the academy's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use *the* Leading Edge Academies Trust's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the academy will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the Leading Edge Academies Trust's sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Principal.

13. Photographs and videos

As part of the Leading Edge Academies Trust's activities, we may take photographs and record images of individuals within our academies.
We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials.
Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within each academy on notice boards and in academy magazines, brochures, newsletters, etc.

- Outside of each academy by external agencies such as the school photographer, newspapers, campaigns
- Online on each academy website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
See photography and video policy for more information on our use of photographs and videos.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our academy and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the academy offices
- Passwords that are at least 8 characters long containing letters and numbers are used to access academy computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for academy-owned equipment (see acceptable usage policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

The Leading Edge Academies Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.
When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an academy context may include, but are not limited to:

- A non-anonymised dataset being published on any Leading Edge Academies Trust member's website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person

- The theft of a academy laptop containing non-encrypted personal data about pupils

18. Training

All staff and trustees are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Leading Edge Academies Trust's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.
This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our academy's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Board of Trustees.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable usage policy
- Photographic and video policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Principal, CEO and the Chair of Trustees
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on a secure area of the academy's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on a secure area of the academy's computer system.

The DPO and Head of School will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will ask the IT department to carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- Details of pupil premium interventions for named children being published on the academy website
- Non-anonymised pupil exam results or staff pay information being shared with governors, notwithstanding our legal duty within our annual report and financial statement
- A academy laptop containing non-encrypted sensitive personal data being stolen or hacked

Appendix 2- Retention guidance

1 Child Protection

These retention periods should be used in conjunction with the document "Safeguarding Children and Safer Recruitment in Education" which can be downloaded from www.everychildmatters.gov.uk.

	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
1.1	*Child Protection files*	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years[1]	SHRED	Child Protection information must be copied and sent under separate cover to new school/college whilst the child is still under 18 (i.e. the information does not need to be sent to a university for example) Where a child is removed from roll to be educated at home, the file should be copied to the Local Education Authority.
1.2	*Allegation of a child protection nature against a member of staff, including where the allegation is unfounded*	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SHRED	'Keeping children safe in education 2015' give statutory guidance on record keeping; see "Record Keeping" on page 45

[1] This amendment has been made in consultation with the Safeguarding Children Group.

2	Governors					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
2.1	*Minutes*					
	Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives
	Inspection copies	No		Date of meeting + 3 years	SHRED [If these minutes contain any sensitive personal information they should be shredded]	
2.2	*Agendas*	No		Date of meeting	SHRED	
2.3	*Reports*	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
2.4	*Annual Parents' meeting papers*	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
2.5	*Instruments of Government*	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed
2.6	*Trusts and Endowments*	No		Permanent	Retain in school whilst operationally required	Transfer to Archives
2.7	*Action Plans*	No		Date of action plan + 3 years	SHRED	It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period
2.8	*Policy documents*	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

2	Governors					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
2.9	*Complaints files*	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes SHRED routine complaints	
2.10	*Annual Reports required by the Department for Education and Skills*	No		Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
2.11	*Proposals for schools to become, or be established as Specialist Status schools*	No			Current year + 3 years	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

3	Management					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
3.1	*Log Books*	Yes[2]		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
3.2	*Minutes of the Senior Management Team and other internal administrative bodies*	Yes[1]		Date of meeting + 5 years	Retain in the school for 5 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

[2] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual pupils and members of staff will become subject to the Data Protection Act 1998.

3	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	*Reports made by the head teacher or the management team*	Yes[1]		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
3.4	*Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities*	Yes[1]		Closure of file + 6 years	SHRED	
3.5	*Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities*	No		Date of correspondence + 3 years	SHRED	
3.6	*Professional development plans*	Yes		Closure + 6 years	SHRED	
3.7	*School development plans*	No		Closure + 6 years	Review	Offer to the Archives
3.8	*Admissions – if the admission is successful*	Yes		Admission + 1 year	SHRED	
3.9	*Admissions – if the appeal is unsuccessful*	Yes		Resolution of case + 1 year	SHRED	
3.10	*Admissions – Secondary Schools – Casual*	Yes		Current year + 1 year	SHRED	
3.11	*Proofs of address supplied by parents as part of the admissions process*	Yes		Current year + 1 year	SHRED	

4	Pupils					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
4.1	*Admission Registers*	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives

4 Pupils						
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
4.2	*Attendance registers*	Yes		Date of register + 3 years	SHRED [If these records are retained electronically any back up copies should be destroyed at the same time]	
4.3	*Pupil record cards*	Yes				
4.3a	*Primary*			N/A		
4.3b	*Secondary*		Limitation Act 1980	DOB of the pupil + 25 years[3]	SHRED	
4.4	*Pupil files*	Yes				
4.4a	*Primary*			N/A		
4.4b	*Secondary*		Limitation Act 1980	DOB of the pupil + 25 years[4]	SHRED	
4.5	*Special Educational Needs files, reviews and Individual Education Plans*	Yes		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum 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.	SHRED	
4.6	*Letters authorising absence*	No		Date of absence + 2 years	SHRED	

[3] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service

[4] As above

4 Pupils						
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
4.7	*Absence books*			Current year + 6 years	SHRED	
4.8	*Examination results*	Yes				
4.8a	*Public*	No		Year of examinations + 6 years	SHRED	Any certificates left unclaimed should be returned to the appropriate Examination Board
4.8b	*Internal examination results*	Yes		Current year + 5 years[5]	SHRED	
4.9	*Any other records created in the course of contact with pupils*	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SHRED	
4.10	*Statement maintained under The Education Act 1996 - Section 324*	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SHRED unless legal action is pending	
4.11	*Proposed statement or amended statement*	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SHRED unless legal action is pending	
4.12	*Advice and information to parents regarding educational needs*	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SHRED unless legal action is pending	

[5] If these records are retained on the pupil file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

4	Pupils					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
4.13	*Accessibility Strategy*	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SHRED unless legal action is pending	
4.14	*Children's SEN Files*	Yes		DOB of pupil + 25 years then review – it may be appropriate to add an additional retention period in certain cases	SHRED unless legal action is pending	
4.15	*Parental permission slips for school trips – where there has been no major incident*	Yes		Conclusion of the trip	SHRED	
4.16	*Parental permission slips for school trips – where there has been a major incident*	Yes	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SHRED	
4.17	*Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools*	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 14 years[6]	N	SHRED or delete securely

[6] This retention period has been set in agreement with the Safeguarding Children's Officer

4	Pupils					
	Basic file description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
4.18	*Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools*	N	3 part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years[7]	N	SHRED or delete securely
4.19	*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	SHRED [If these records are retained electronically any back up copies should be destroyed at the same time]	

5	Curriculum				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
5.1	*Curriculum development*	No		Current year + 6 years	SHRED
5.2	*Curriculum returns*	No		Current year + 3 years	SHRED
5.3	*School syllabus*	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.4	*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 new retention period or SHRED
5.5	*Timetable*	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.6	*Class record books*	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED

5	Curriculum				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
5.7	*Mark Books*	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.8	*Record of homework set*	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.9	*Pupils' work*	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SHRED
5.10	*Examination results*	Yes		Current year + 6 years	SHRED
5.11	*SATS records*	Yes		Current year + 6 years	SHRED
5.12	*PAN reports*	Yes		Current year + 6 years	SHRED
5.13	*Value added records*	Yes		Current year + 6 years	SHRED

6	Personnel Records held in Schools				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
6.1	*Timesheets, sick pay*	Yes	Financial Regulations	Current year + 6 years	SHRED
6.2	*Staff Personal files*	Yes		Termination + 7 years	SHRED
6.3	*Interview notes and recruitment records*	Yes		Date of interview + 6 months	SHRED
6.4	*Pre-employment vetting information (including CRB checks)*	No	CRB guidelines	Date of check + 6 months	SHRED [by the designated member of staff]
6.5	*Disciplinary proceedings:*	Yes	Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.		
6.5a	*oral warning*			Date of warning + 6 months	SHRED[7]
6.5b	*written warning – level one*			Date of warning + 6 months	SHRED
6.5c	*written warning – level two*			Date of warning + 12 months	SHRED

[7] If this is placed on a personal file it must be weeded from the file.

6	Personnel Records held in Schools				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
6.5d	*final warning*			Date of warning + 18 months	SHRED
6.5e	*case not found*			If child protection related please see 1.2 otherwise shred immediately at the conclusion of the case	SHRED
6.6	*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	SHRED
6.7	*Annual appraisal/assessment records*	No		Current year + 5 years	SHRED
6.8	*Salary cards*	Yes		Last date of employment + 85 years	SHRED
6.9	*Maternity pay records*	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SHRED
6.10	*Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995*	Yes		Current year + 6 years	SHRED
6.11	*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.	

7	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
7.1	*Accessibility Plans*		Disability Discrimination Act	Current year + 6 years	SHRED

7	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
7.2	*Accident Reporting*		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	*Adults*	Yes		Date of incident + 7 years	SHRED
7.2b	*Children*	Yes		DOB of child + 25 years[8]	SHRED
7.3	*COSHH*			Current year + 10 years [where appropriate an additional retention period may be allocated]	SHRED
7.4	*Incident reports*	Yes		Current year + 20 years	SHRED
7.5	*Policy Statements*			Date of expiry + 1 year	SHRED
7.6	*Risk Assessments*			Current year + 3 years	SHRED
7.7	*Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos*			Last action + 40 years	SHRED
7.8	*Process of monitoring of areas where employees and persons are likely to have come in contact with radiation*			Last action + 50 years	SHRED
7.9	*Fire Precautions log books*			Current year + 6 years	SHRED

[8] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the pupil reaches the age of 25 this retention period has been applied.

8	Administrative					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
8.1	*Employer's Liability certificate*			Closure of the school + 40 years	SHRED	
8.2	*Inventories of equipment and furniture*			Current year + 6 years	SHRED	
8.3	*General file series*			Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
8.4	*School brochure or prospectus*			Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
8.5	*Circulars (staff/parents/pupils)*			Current year + 1 year	SHRED	
8.6	*Newsletters, ephemera*			Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
8.7	*Visitors book*			Current year + 2 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

8	Administrative					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
8.8	*PTA/Old Pupils Associations*			Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

9	Finance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
9.1	*Annual Accounts*		Financial Regulations	Current year + 6 years		Offer to the Archives
9.2	*Loans and grants*		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
9.3	*Contracts*					
9.3a	under seal			Contract completion date + 12 years	SHRED	
9.3b	under signature			Contract completion date + 6 years	SHRED	
9.3c	monitoring records			Current year + 2 years	SHRED	
9.4	*Copy orders*			Current year + 2 years	SHRED	
9.5	*Budget reports, budget monitoring etc*			Current year + 3 years	SHRED	
9.6	*Invoice, receipts and other records covered by the Financial Regulations*		Financial Regulations	Current year + 6 years	SHRED	
9.7	*Annual Budget and background papers*			Current year + 6 years	SHRED	

9	Finance					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
9.8	*Order books and requisitions*			Current year + 6 years	SHRED	
9.9	*Delivery Documentation*			Current year + 6 years	SHRED	
9.10	*Debtors' Records*		Limitation Act 1980	Current year + 6 years	SHRED	
9.11	*School Fund – Cheque books*			Current year + 3 years	SHRED	
9.12	*School Fund – Paying in books*			Current year + 6 years then review	SHRED	
9.13	*School Fund – Ledger*			Current year + 6 years then review	SHRED	
9.14	*School Fund – Invoices*			Current year + 6 years then review	SHRED	
9.15	*School Fund – Receipts*			Current year + 6 years	SHRED	
9.16	*School Fund – Bank statements*			Current year + 6 years then review	SHRED	
9.17	*School Fund – School Journey books*			Current year + 6 years then review	SHRED	
9.18	*Applications for free school meals, travel, uniforms etc*			Whilst child at school	SHRED	
9.19	*Student grant applications*			Current year + 3 years	SHRED	
9.20	*Free school meals registers*	Yes	Financial Regulations	Current year + 6 years	SHRED	
9.21	*Petty cash books*		Financial Regulations	Current year + 6 years	SHRED	

10	Property					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
10.1	*Title Deeds*			Permanent	Permanent these should follow the property unless the property has been registered at the Land Registry	Offer to Archives if the deeds are no longer needed
10.2	*Plans*			Permanent	Retain in school whilst operational	Offer to Archives[9]
10.3	*Maintenance and contractors*		Financial Regulations	Current year + 6 years	SHRED	
10.4	*Leases*			Expiry of lease + 6 years	SHRED	
10.5	*Lettings*			Current year + 3 years	SHRED	
10.6	*Burglary, theft and vandalism report forms*			Current year + 6 years	SHRED	
10.7	*Maintenance log books*			Last entry + 10 years	SHRED	
10.8	*Contractors' Reports*			Current year + 6 years	SHRED	

11	Local Education Authority					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
11.1	*Secondary transfer sheets (Primary)*	Yes		Current year + 2 years	SHRED	
11.2	*Attendance returns*	Yes		Current year + 1 year	SHRED	
11.3	*Circulars from LEA*			Whilst required operationally	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

[9] If the property has been sold for private housing then the archives service will embargo these records for an appropriate period of time to prevent them being used to plan or carry out a crime.

12	Department for Children, Schools and Families					
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
12.1	*HMI reports*			These do not need to be kept any longer		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
12.2	*OFSTED reports and papers*			Replace former report with any new inspection report	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
12.3	*Returns*			Current year + 6 years	SHRED	
12.4	*Circulars from Department for Children, Schools and Families*			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

13	Connexions				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the adminis
13.1	*Service level agreements*			Until superseded	SHRED
13.2	*Work Experience agreement*			DOB of child + 18 years	SHRED

14	Schools Meals				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the adminis
14.1	*Dinner Register*			C + 3 years	SHRED
14.2	*School Meals Summary Sheets*			C + 3 years	SHRED

15	Family Liaison Officers and Parent Support Assistants				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Method of Disposal
15.1	*Day Books*	Y		Current year + 2 years then review	SHRED
15.2	*Reports for outside agencies – where the report has been included on the case file created by the outside agency*	Y		Whilst the child is attending the school then destroy	SHRED
15.3	*Referral forms*	Y		While the referral is current then	SHRED

15	Family Liaison Officers and Parent Support Assistants				
	Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Method of Disposal
15.4	*Contact data sheets*	Y		Current year then review, if contact is no longer active then destroy	SHRED
15.5	*Contact database entries*	Y		Current year then review, if contact is no longer active then destroy	DELETE
15.6	*Group Registers*	Y		Current year + 2 years	SHRED