

# Data Protection Policy

## Ladbroke JMI School



**Approved by:** Resources Committee

**Date:** 20<sup>th</sup> June

**Last reviewed on:** June 2018

**Next review due by:** June 2019

## Contents

1. Aims.....	2
2. Legislation and guidance .....	2
3. Definitions .....	3
4. The data controller .....	4
5. Roles and responsibilities .....	4
6. Data protection principles.....	5
7. Collecting personal data.....	5
8. Sharing personal data .....	5
9. Subject access requests and other rights of individuals .....	6
10. Parental requests to see the educational record .....	8
11. CCTV .....	8
12. Photographs and videos .....	8
13. Data protection by design and default .....	8
14. Data security and storage of records.....	9
15. Disposal of records .....	9
16. Personal data breaches .....	9
17. Training.....	9
18. Monitoring arrangements .....	10
20. Links with other policies .....	10
Appendix 1: Personal data breach procedure .....	11
Appendix 2: Subject Access Forms and Data Amendment Form .....	13
Appendix 3: Data Retention Schedule.....	15
Appendix 4: DPO Job Description .....	
.....	

### 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, 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 also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

### 3. Definitions

Term	Definition
<p><b>Personal data</b></p>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<p><b>Special categories of personal data</b></p>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> <li>• Criminal records</li> </ul>
<p><b>Processing</b></p>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<p><b>Data subject</b></p>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<p><b>Data controller</b></p>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<p><b>Data processor</b></p>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>

<b>Personal data breach</b>	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

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school 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 school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

### 5.1 Governing board

The governing board has overall responsibility for ensuring that our school 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 governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **Mr. Mark Turner** and is contactable via **dpo@ladbrooke.herts.sch.uk**

### 5.3 Headteacher

The headteacher acts as the representative of the data controller 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 school 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 school 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 school 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 school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school 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 school, 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 school 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.

### 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 school's retention schedule which follows recommendations from the [Information and Records Management Society's toolkit for schools](#) (See appendix 3)

## 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 government bodies 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 school 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 using the subject access request form which can be found in appendix 2 of this document or be downloaded from the website.

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 below the age of 12 are generally not 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 school may 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

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

## 11. CCTV

We use CCTV in various locations around the school site 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 the Headteacher.

## 12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice/display boards and in school magazines, brochures, newsletters, etc.
- Within schools in books to show work/learning complete
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school 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 our e-Safety policy for more information on our use of photographs and videos.

## 13. 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 school'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 school 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

## 14. 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 school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school 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 and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our e-safety 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)

## 15. 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

## 16. Personal data breaches

The school 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 a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school 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 school laptop containing non-encrypted personal data about pupils

## 17. Training

All staff and governors 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 school's processes make it necessary.

## **18. 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 school's practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing body.

## **20. Links with other policies**

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-Safety
- Child Protection/Safeguarding

## 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 headteacher and the chair of governors
- 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 [\[set out where you keep records of these decisions – for example, on the school's computer system, or on a designated software solution\]](#)
- 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 the main computer system

- The DPO and headteacher 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 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

*Other types of breach that you might want to consider could include:*

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*

## Appendix 2: Subject Access Request Forms

### Subject Access Request Form

Child's Details	
Child's name	
Child's date of birth	
Child's current address	
Child's current class	
Person Requesting Data Review	
Your name	
Your relationship to the child	
Your address	
Your telephone number	
Do you have parental responsibility?	
Your Request	
What data/which records to you wish to view?	
Why do you wish to view them?	
What do you expect to find in these records?	

**Signed :** ..... **Date :** .....

Once completed, please hand this form into the school office who will ensure that it is forwarded to the right person (the school's Data Protection officer). We are required to respond to your request within one calendar month of this request being received.

*GDPR: This form will be kept until the request has been completed. Once this has occurred, the form will be destroyed although a summary of the request and outcome will be kept on file for monitoring and reporting purposes*

## Data Amendment Request Form

Child's Details	
Child's name	
Child's date of birth	
Child's current address	
Child's current class	
Person Requesting Data Amendment	
Your name	
Your relationship to the child	
Your address	
Your telephone number	
Do you have parental responsibility?	
Your Request	
What data/which records do you wish to have amended?	
What amendments do you want? Do you want it updating, amending or deleting?	
Why do you want these changes undertaken?	

**Signed:** ..... **Date:** .....

Once completed, please hand this form into the school office who will ensure that it is forwarded to the right person (the school's Data Protection officer). We are required to respond to your request within one calendar month of this request being received.

*GDPR: This form will be kept until the request has been completed. Once this has occurred, the form will be destroyed although a summary of the request and outcome will be kept on file for monitoring and reporting purposes*

## Appendix 3: Data Retention Schedule

This information is taken for the Information management Toolkit for Schools ([www.irms.org.uk](http://www.irms.org.uk))

1.1 Governing Body					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.1.1	Agendas and Minutes for Governing Body meetings including <ul style="list-style-type: none"> <li>- Principal set (signed)</li> <li>- Copies of reports linked to meetings</li> <li>- Part II discussions (stored separately)</li> </ul>	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 <sup>1</sup>
1.1.2	Instruments of Government including Articles of Association	No		Current version kept permanently, old version destroyed when replaced	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.3	Policy documents created and administered by the Governing Body	No		Life of the policy	SECURE DISPOSAL
1.1.4	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
1.2 Head teacher and Senior Management Team					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.1	Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Until the end of next academic year (or longer if deemed necessary)	SECURE DISPOSAL

## 1.2 Head teacher and Senior Management Team

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.2.2	Reports created by the Head Teacher Management or admin Team E.g. team meetings, monitoring records, subject action plans, attendance	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + up to 3 years then review	SECURE DISPOSAL
1.2.3	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 review (unless there is no lawful reason for keeping the correspondence)	SECURE DISPOSAL
1.2.4	School Improvement Plans	No		Life of the plan + 3 years	SECURE DISPOSAL
1.2.5.	Premises Maintenance Plan	No		Current Plan retained until updated version available	SECURE DISPOSAL

## 1.3 Admissions Process

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.1	All records relating 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	SECURE DISPOSAL

### 1.3 Admissions Process

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.3.2	Admissions (Nursery) – if the admission is successful	Yes		Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions (Nursery) – if the appeal is unsuccessful	Yes		Resolution of case	SECURE DISPOSAL
1.3.4	Register of Admissions	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Admission register is kept on SIMS for 6 years after the child leaves	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	Proofs of address supplied by parents as part of the admissions process	Yes		Until admission process has been completed	SECURE DISPOSAL
1.3.6	Supplementary Information form including additional information such as religion, medical conditions etc.	Yes		This information is added to the pupil file (successful) Until appeals process completed (unsuccessful)	SECURE DISPOSAL ON LEAVING SCHOOL. ELECTRONIC RECORD SENT TO NEXT SCHOOL

## 1.4 Operational Administration

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
1.4.1	Records relating to the creation and publication of the school brochure or	No		Current year + 3 years	STANDARD DISPOSAL
1.4.2	Newsletters and circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.3	Visitors' Books and Signing in Sheets	Yes		Current year + 6 years	SECURE DISPOSAL
1.4.4	Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Retained until updated version	SECURE DISPOSAL

## 2.1 Recruitment

	Basic file description	Data Protection 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 head teacher	Yes		Date of appointment + 6 years (held by Hertfordshire recruitment team)	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 Recruitment					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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	
2.1.6	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom <sup>4</sup>	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	
2.2 Operational Staff Management					
	Basic file description	Data Protection 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	Annual appraisal records	Yes		Current year + 5 years	SECURE DISPOSAL

### 2.3 Management of Disciplinary and Grievance Processes

Basic file description	Data Protection 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 <sup>5</sup>	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	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.	SECURE DISPOSAL These records must be shredded
2.3.2 Disciplinary Proceedings	Yes			
oral warning			Date of warning <sup>6</sup> + 6 months	
written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
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

### 2.4 Health and Safety

Basic file description	Data Protection 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		Current policy retained permanently	SECURE DISPOSAL
2.4.2 Health and Safety Risk Assessments	No		Current versions retained, updated either annually or every 3 years	SECURE DISPOSAL

## 2.4 Health and Safety

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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	Adult -Date of the incident + 6 years Child - 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 SI 1012 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 log books	No		Current year + 6 years	SECURE DISPOSAL

## 2.5 Payroll and Pensions

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
2.5.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL

## 3.1 Risk Management and Insurance

	Basic file description	Data Protection 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		Current certificate retained	SECURE DISPOSAL

## 3.2 Asset Management

	Basic file description	Data Protection 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 Protection 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	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 Protection 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	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 copy retained, updated annually	SECURE DISPOSAL

### 3.5 School Fund

	Basic file description	Data Protection 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 Protection 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

### 4.1 Property Management

	Basic file description	Data Protection 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	

Basic file description		Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
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	Information relating to leases	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 Protection 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		Retained until the end of the academic year	SECURE DISPOSAL
4.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Retained until the end of the academic year	SECURE DISPOSAL

## 5.1 Pupil's Educational Record

Basic file description		Data Protection 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	Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school.

## 5.1 Pupil's Educational Record

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
5.1.2	Examination Results – Pupil Copies Public and Internal	Yes		This information should be added to the pupil file	
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

## 5.2 Attendance

	Basic file description	Data Protection 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 authorised absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

## 5.3 Special Educational Needs

	Basic file description	Data Protection Issues	Statutory Provisions		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 Act 2001 Section 14	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

## 6.1 Statistics and Management Information

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
6.1.1	Examination Results (Schools Copy)	Yes		<p>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.</p> <p>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</p>	SECURE DISPOSAL
6.1.2	Examination Papers (KS1 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	SEF	Yes		Current copy retained until updated version available	SECURE DISPOSAL

6.2 Implementation of Curriculum					
	Basic file description	Data Protection 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	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	
6.2.3	Class Record Books	No		Current year	
6.2.4	Mark Books	No		Current year	
6.2.5	Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year (unless agreed to keep for use in school)	

7.1 Educational Visits outside the Classroom					
	Basic file description	Data Protection 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 <a href="http://oeapng.info">http://oeapng.info</a> specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL
7.1.2	Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL

7.1.3	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	
-------	--	-----	---------------------------------	---	--

8.1 Local Authority					
	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at the end of the administrative life of the record
8.1.1	Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.2	School Census Returns	No		Current year + 5 years	SECURE DISPOSAL

8.2 Central Government					
	Basic file description	Data Protection 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



## Model role description – data protection officer

---

### Purpose

The DPO is responsible for monitoring compliance with current data protection law, and has the knowledge, support and authority to do so effectively. They oversee the school's data protection processes and advise the school on best practice.

### Key responsibilities

To:

- Advise the school and its employees about their obligations under current data protection law, including the General Data Protection Regulation (GDPR)
- Develop an in-depth understanding of the school's processing operations, information systems, data security processes and needs, and administrative rules and procedures
- Monitor the school's compliance with data protection law, by:
  - Collecting information to identify data processing activities
  - Analysing and checking the compliance of data processing activities
  - Informing, advising and issuing recommendations to the school
  - Ensuring they remain an expert in data protection issues and changes to the law, attending relevant training as appropriate
- Ensure the school's policies are followed, through:
  - Assigning responsibilities to individuals
  - Awareness-raising activities
  - Co-ordinating staff training
  - Conducting internal data protection audits
- Advise on and assist the school with carrying out data protection impact assessments, if necessary
- Act as a contact point for the Information Commissioner's Office (ICO), assisting and consulting it where necessary, including:
  - Helping the ICO to access documents and information
  - Seeking advice on data protection issues
- Act as a contact point for individuals whose data is processed (for example, staff, pupils and parents), including:
  - Responding to subject access requests
  - Responding to other requests regarding individuals' rights over their data and how it is used
- Take a risk-based approach to data protection, including:
  - Prioritising the higher-risk areas of data protection and focusing mostly on these
  - Advising the school if/when it should conduct an audit, which areas staff need training in, and what the DPO role should involve
- Report to the *[governing board/board of trustees]* on the school's data protection compliance and associated risks
- Respect and uphold confidentiality, as appropriate and in line with data protection law, in carrying out all duties of the role
- Undertake any additional tasks necessary to keep the school compliant with data protection law and be successful in the role
- Work with external stakeholders, such as suppliers or members of the community, on data protection issues

## Person specification

Criteria	Desirable qualities
<b>Qualifications</b>	<ul style="list-style-type: none"> <li>• Background in information security, data protection or IT desired</li> <li>• Educated to degree level, or equivalent professional experience</li> <li>• Relevant data protection qualification desired</li> </ul> <p><i>[You will need to use your own judgement to determine the qualifications your DPO needs to have, depending on your data protection needs]</i></p>
<b>Experience</b>	<ul style="list-style-type: none"> <li>• Professional experience of data protection law</li> <li>• Experience of managing data protection compliance, particularly responding to subject access requests</li> </ul> <p><i>[You will need to use your own judgement to determine the experience your DPO needs to have, depending on your data protection needs]</i></p>
<b>Skills and knowledge</b>	<ul style="list-style-type: none"> <li>• Knowledge of data protection law (the GDPR and Data Protection Act 1998)</li> <li>• Knowledge of information security and data processing principles and good practice</li> <li>• An understanding, and prior use of the following systems:               <ul style="list-style-type: none"> <li>○ <i>[Insert any data systems your school uses e.g. MIS, computer operating systems, data security systems]</i></li> </ul> </li> <li>• Excellent communication skills</li> <li>• Excellent teamwork and interpersonal skills, with proven ability to maintain relationships across a school or other organisation</li> <li>• Ability to explain complex data protection and information security information to a non-specialist audience</li> </ul>
<b>Personal qualities</b>	<ul style="list-style-type: none"> <li>• Detail-oriented</li> <li>• Ability to work under pressure</li> <li>• Ability to prioritise tasks effectively</li> <li>• Ability to work independently and autonomously with minimal supervision</li> <li>• Commitment to maintaining confidentiality at all times</li> </ul>