



# HUNDON AND THURLOW PRIMARY FEDERATION

## Data Protection Policy

**Approved by:** Chair Of Governors **Date:** May 2018

**Last reviewed on:** May 2018

**Next review due  
by:** Spring 2020

# 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 .....	4
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.....	7
11. Photographs and videos .....	8
12. Data protection by design and default .....	8
13. Data security and storage of records.....	8
14. Disposal of records .....	9
15. Personal data breaches.....	9
16. Training .....	9
17. Monitoring arrangements .....	9
18. Links with other policies .....	10
19. Appendix 1: Subject Access Request Form .....	11
Appendix 2: Personal data breach procedure .....	13-15
Appendix 3: Document Retention Schedule.....	

## 1. Aims

Our schools 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](#).

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
<b>Personal data</b>	<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>
<b>Special categories of personal data</b>	<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>• Health - physical or mental</li><li>• Sex life or sexual orientation</li></ul>

<b>Processing</b>	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.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<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 schools process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The schools are 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 schools, 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 schools comply 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 [Sara Clark](mailto:saraclarkdpo@hundonschool.co.uk) and is contactable via email at [saraclarkdpo@hundonschool.co.uk](mailto:saraclarkdpo@hundonschool.co.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 schools can **fulfil a contract** with the individual, or the individual has asked the schools to take specific steps before entering into a contract

- The data needs to be processed so that the schools 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 schools, 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 schools 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 (except for online counselling and preventive services).

## 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 can be found as an appendix to this policy - **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 schools hold 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, email or fax 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. A template form is included in this policy as **Appendix 1**.

### 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 schools 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. 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 boards and in school magazines, brochures, newsletters, etc.
- 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 [safeguarding policy](#) for more information on our use of photographs and videos.

## 12. 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

### 13. 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 [Information Management 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)

### 14. 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.

### 15. Personal data breaches

The schools 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 2**.

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

## 16. 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.

## 17. 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 2 years** and shared with the full governing board.

## 18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Information Management Policy
- Safeguarding Policy

## 19. Appendices

- Appendix 1. Subject Access Request Form
- Appendix 2. Personal Data Breach Procedure
- Appendix 3. Data Retention Schedule



## Appendix 1: Subject Access Request Form

Date:

*Hundon and Thurlow Primary Federation*

**Re: subject access request**

Dear *Sara Clark*

Please provide me with the information about me that I am entitled to under the General Data Protection Regulation. This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer  Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: <i>Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:</i> <ul style="list-style-type: none"><li>• <i>Your personnel file</i></li><li>• <i>Your child's medical records</i></li><li>• <i>Your child's behavior record, held by [insert class teacher]</i></li><li>• <i>Emails between 'A' and 'B' between [date]</i></li></ul>

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

## Appendix 2: 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 is 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 the school'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 the school's 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 coordinator 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*

#### ***Non-anonymised pupil exam results or staff pay information being shared with governors***

- *If Non-anonymised pupil exam results or staff pay information is accidentally made available to governors, the information must be re-called as soon as we become aware of the error*
- *Members of the governing body who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *In any cases where the recall of information is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the information, explain that the information was sent in error, and request that those individuals delete/destroy 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*

#### ***A school laptop containing non-encrypted sensitive personal data being stolen or hacked***

- *Members of staff must alert the sender and the DPO as soon as they become aware of the incident*
- *The DPO will contact the school ICT coordinator for further guidance on how to limit data loss*





## Appendix 3: Data Retention Schedule

*\*This retention schedule is based on guidance from the information records management society: <http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school>.*

*It encompasses records managed by all types of school - some of the file descriptions listed may not be relevant to every school.*

1 Child Protection							
These retention periods should be used in conjunction with the document <u>Keeping children safe in education</u>							
	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
1.1	Child protection files	Yes	Education Act 2002, s175 <u>Education Act 2002</u>	DOB + 25 years [1]	SHRED or delete securely	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)	OFFICIAL SENSITIVE
1.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	<u>Employment Practices Code: Supplementary Guidance</u> 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance <u>Keeping children safe in education</u>	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer		<u>Keeping children safe in education</u> p35 (Record Keeping)	OFFICIAL SENSITIVE

## 2 Governors

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
2.2	Minutes Inspection copies	No		Date of meeting + 3 years	SHRED or delete securely		OFFICIAL
2.3	Agendas	No		Date of meeting	SHRED		OFFICIAL
2.4	Reports	No		Date of meeting + 6 years	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
2.5	Annual Patents' meeting papers	No		Date of meeting + 6 years	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
2.6	Trusts and Endowments	No		Permanent <i>(Retain in school whilst operationally required)</i>	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
2.7	Action plans	No		Date of meeting + 3 years	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
2.8	Statutory policy documents	No		Expiry of policy <i>(Retain in school whilst operationally</i>	SHRED	Consider transferring to <u>Archives</u> if part of a past decision making process	OFFICIAL

				required)			
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first 6 years  Review for further retention in the case of contentious disputes  SHRED (or delete securely) routine complaints		OFFICIAL-SENSITIVE
2.10	Proposals for schools to become, or be established as Specialist Status schools	No		Current year + 3 years	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL

### 3 Management

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
3.1	Log books	Yes [1]		Date of last entry in the book + 6 years	Retain in school for 3 years from date of entry	Consider transferring to <u>Archives</u>	OFFICIAL
3.2	Minutes of the Senior Management Team and other internal administrative bodies	Yes [1]		Date of last entry in the book + 5 years	Retain in school for 5 years from date of meeting	Consider transferring to <u>Archives</u>	OFFICIAL
3.3	Reports made by the Head Teacher or the Management Team	Yes [1]		Date of last entry in the book + 3 years	Retain in school for 3 years from date of meeting	Consider transferring to <u>Archives</u>	OFFICIAL
3.4	Records created by Head Teacher or other members of staff with administrative responsibilities	Yes [1]		Closure of file + 6 years	SHRED or delete securely		OFFICIAL
3.5	Correspondence created by Head Teacher or other	No		Date of correspondence +	SHRED or delete		OFFICIAL

	members of staff with administrative responsibilities			3 years	securely		
3.6	Professional development places	Yes		Closure + 6 years	SHRED or delete securely		OFFICIAL
3.7	School development plans	No		Closure + 6 years		Consider transferring to <u>Archives</u>	OFFICIAL
3.8	Admissions - <i>Successful</i>	Yes		Resolution of case + 1 year	SHRED		OFFICIAL-SENSITIVE
3.9	Admissions - <i>Unsuccessful at appeal</i>	Yes		Current year + 1 year	SHRED or delete securely		OFFICIAL-SENSITIVE
3.10	Admissions - Secondary Schools - <i>Casual</i>	Yes		Current year + 1 year	SHRED or delete securely		OFFICIAL-SENSITIVE
3.11	Proofs of address (supplied by parents as part of admissions process)	Yes		Current year + 1 year	SHRED or delete securely		OFFICIAL-SENSITIVE

#### 4 School

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
4.1	Admission registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in school for 6 years from date of the last entry	Consider transferring to <u>Archives</u>	OFFICIAL-SENSITIVE
4.2	Attendance registers	Yes	<u>The Education (Pupil Registration) (England) Regulations 2006 (No. 1751)</u>	Date of register + 3 years	SHRED or delete securely		OFFICIAL-SENSITIVE
4.3	Pupil record cards - Primary	Yes		Retain for the time which the pupil remains at the primary school	Transfer to secondary school (or other primary school) when the child leaves the school.  In the case of exclusion it may be necessary to transfer the record to the appropriate service.		OFFICIAL-SENSITIVE

4.4	Pupil record cards - Secondary	Yes	<u>Limitation Act 1980</u>	DOB of the pupil + 25 years	SHRED or delete securely		OFFICIAL-SENSITIVE
4.5	Pupil files - Primary	Yes		Retain for the time which the pupil remains at the primary school	Transfer to secondary school (or other primary school) when the child leaves the school.  In the case of exclusion it may be necessary to transfer the record to the appropriate service.		OFFICIAL-SENSITIVE
4.6	Pupil files - Secondary	Yes	<u>Limitation Act 1980</u>	DOB of the pupil + 25 years	SHRED or delete securely		OFFICIAL-SENSITIVE
4.7	Special Education Needs files, reviews and Individual Education plans	Yes		DOB of the pupil + 25 years	SHRED or delete securely		OFFICIAL-SENSITIVE
4.8	Letters	No		Date of absence +	SHRED or		OFFICIAL



	authorising absence			2 years	delete securely		
4.9	Absence books	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
4.10	Examination results - <i>Public</i>	No		Year of examination + 6 years	SHRED or delete securely	Any certifications left unclaimed should be returned to the appropriate Examinations Board	OFFICIAL
4.11	Examination results - <i>Internal</i>	Yes		Current year + 5 years	SHRED or delete securely		OFFICIAL
4.12	Any other records created in the course of contact with pupils	Yes		Current year + 3 years	Review at end - allocate a further retention period or SHRED		OFFICIAL-SENSITIVE
4.13	Statement maintained under the Education Act 1996 - section 324	Yes	<u>Special Educational Needs and Disability Act 2001</u> (section 1)	DOB + 30 years	SHRED or delete securely - unless legal action is pending		OFFICIAL-SENSITIVE
4.14	Proposed statement or amended	Yes	<u>Special Educational Needs and Disability Act</u>	DOB + 30 years	SHRED or delete		OFFICIAL-SENSITIVE

	statement		<u>2001</u> (section 1)		securely - unless legal action is pending		
4.1 5	Advice and information to parents regarding educational needs	Yes	<u>Special Educational Needs and Disability Act 2001</u> (section 2)	Closure + 12 years	SHRED or delete securely - unless legal action is pending		OFFICIAL-SENSITIVE
4.1 6	Accessibility strategy	Yes	<u>Special Educational Needs and Disability Act 2001</u> (section 14)	Closure + 12 years	SHRED or delete securely - unless legal action is pending		OFFICIAL-SENSITIVE
4.1 7	Children's SEN files	Yes		DOB of pupil + 25 years	SHRED or delete securely - unless legal action is pending		OFFICIAL-SENSITIVE
4.1 8	Parental permission slips for school trips  - where there has been no major incident	Yes		Conclusion of the trip	SHRED or delete securely		OFFICIAL-SENSITIVE

4.1 9	Parental permission slips for school trips  - where there has been a major incident	Yes	<u>Limitation Act 1980</u>	DOB of the pupil involved + 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 or delete securely		OFFICIAL-SENSITIVE
4.2 0	Records created by schools to obtain approval to run an Educational Visit outside the Classroom  - Primary Schools	No	3 part supplement to the <u>Health &amp; Safety of Pupils on Educational visits (HASPEV) (1998)</u>	Date of visit + 14 years	SHRED or delete securely		OFFICIAL
4.2 1	Records created by schools to obtain approval to run an	No	3 part supplement to the <u>Health &amp; Safety of Pupils on Educational visits (HASPEV) (1998)</u>	Date of visit + 10 years	SHRED or delete securely		OFFICIAL

	Educational Visit outside the Classroom  - <i>Secondary Schools</i>						
4.2 2	Dinner Register	Yes		Current year + 3 years	SHRED or delete securely		OFFICIAL
4.2 3	School meals summary sheets	Yes		Current year + 3 years	SHRED or delete securely		OFFICIAL
4.2 4	Walking Bus registers	Yes		Date of register + 3 years	SHRED or delete securely		OFFICIAL-SENSITIVE

5 Curriculum							
	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
5.1	Curriculum development	No		Current year + 6 years	SHRED		OFFICIAL
5.2	Curriculum returns	No		Current year + 3 years	SHRED		OFFICIAL
5.3	Schools syllabus	No		Current year + 1 year	Review at end - allocate a further retention		OFFICIAL

					period or SHRED		
5.4	Schemes of work	No		Current year + 1 year	Review at end - allocate a further retention period or SHRED		OFFICIAL
5.5	Timetable	No		Current year + 1 year	Review at end - allocate a further retention period or SHRED		OFFICIAL
5.6	Class record books	No		Current year + 1 year	Review at end - allocate a further retention period or SHRED		OFFICIAL
5.7	Mark books	No		Current year + 1 year	Review at end - allocate a further retention period or SHRED		OFFICIAL
5.8	Record of homework set	No		Current year + 1 year	Review at end - allocate a further retention		OFFICIAL

					period or SHRED		
5.9	Pupil's work	No		Current year + 1 year	Review at end - allocate a further retention period or SHRED		OFFICIAL
5.10	Examination results	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
5.11	SATS records	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
5.12	PAN records	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
5.13	Value added records	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE

6 Curriculum							
	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
6.1	Timesheets, sick pay	Yes	<u>Financial regulations</u>	Current year + 6 years	SHRED or delete		OFFICIAL

					securely		
6.2	Staff personal files	Yes		Termination + 7 years	SHRED or delete securely		OFFICIAL
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SHRED or delete securely		OFFICIAL
6.4	Pre-employment vetting information (including DBS checks)	Yes	<u>DBS guidelines</u>	Date of check + 6 months	SHRED or delete securely		OFFICIAL
6.5	Single Central Record	Yes	<u>ISA guidelines</u>	Keep until school closure	Consider transferring to Archives or SHRED or delete securely		OFFICIAL
6.6	Disciplinary proceedings	Yes	Where the warning relates to child protection issues see <u>1.2</u> . If the disciplinary proceedings relate to a child protection matter, contact your safeguarding children offer for further advice.				OFFICIAL-SENSITIVE
6.6a	Disciplinary proceedings - Warning - oral	Yes		Date of warning + 6 months	SHRED or delete securely		OFFICIAL
6.6b	Disciplinary proceedings -	Yes		Date of warning + 6 months	SHRED or delete		OFFICIAL

	Warning - <i>written (level one)</i>				securely		
6.6c	Disciplinary proceedings - Warning - <i>written (level two)</i>	Yes		Date of warning + 12 months	SHRED or delete securely		OFFICIAL
6.6d	Disciplinary proceedings - Warning - <i>final</i>	Yes		Date of warning + 18 months	SHRED or delete securely		OFFICIAL
6.6e	Disciplinary proceedings - Warning - <i>case not found</i>	Yes	Where the warning relates to child protection issues see <u>1.2</u> . Otherwise immediately at conclusion of case SHRED or delete securely				OFFICIAL-SENSITIVE
6.7	Annual appraisal - assessment records	Yes		Current year + 5 years	SHRED or delete securely		OFFICIAL
6.8	Salary records	Yes		SHRED or delete securely			OFFICIAL
6.9	Maternity pay records	Yes	<u>Statutory Maternity Pay (SMP) - General Information</u>	Current year + 3 years	SHRED or delete securely		OFFICIAL
6.10	Records held under <u>Retirement Benefits Schemes (Information</u>	Yes		Current year + 6 years	SHRED or delete securely	<i>If this is placed in the personal file it must be weeded out.</i>	OFFICIAL



	<u>Powers) Regulations 1995</u>						
--	---------------------------------	--	--	--	--	--	--

7 Health & Safety							
	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
7.1	Accessibility plans	No	<u>Disability Discrimination Act 2005</u>	Current year +6 years	SHRED		OFFICIAL
7.2	Accident reporting	No	<u>Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980.</u>				
7.2a	Accident reporting- - Adults (all accidents)	Yes		Date of incident +7 years	SHRED or delete securely		OFFICIAL-SENSITIVE
7.2b	Accident reporting- - Children (all accidents)	Yes		DOB of child + 25 years	SHRED or delete securely		OFFICIAL-SENSITIVE
7.3	<u>COSHH</u>	No		Current year + 10 years	SHRED	Review for further retention where appropriate	OFFICIAL
7.4	Incident reports	Yes		Current year + 20 years	SHRED or delete securely		OFFICIAL-SENSITIVE

7.5	Policy statements	No		Date of expiry + 1 year	SHRED		OFFICIAL
7.6	Risk assessments	No		Current year +3 years	SHRED		OFFICIAL
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No		Last action + 40 years	SHRED		OFFICIAL
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation	No		Last action + 40 years	SHRED		OFFICIAL
7.9	Fire Precautions log books	No		Current year + 6 years	SHRED		OFFICIAL

## 8 Administrative

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record	Protective marking classification
8.1	Employer's liability certificate	No		Closure of the school + 40 years	SHRED	OFFICIAL

8.2	Inventories of equipment and furniture	No		Current year +6 years	SHRED		OFFICIAL
8.3	General administrative records <i>(records not specifically listed elsewhere)</i>	No		Current year + 5 years	Review to see if further retention is needed or SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
8.4	School brochure or prospectus	No		Current year + 3 years	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
8.5	Circulars (staff / parents / pupils)	No		Current year + 1 year	SHRED		OFFICIAL
8.6	Newsletters, ephemera	No		Current year + 1 years	Review to see if further retention is needed - or SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
8.7	Visitors book	Yes		Current year + 2 years	Review to see if further retention is needed or SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL

8.8	PTA / Old pupils associations	Yes		Current year + 6 years	Review to see if further retention is needed or SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL
-----	-------------------------------	-----	--	------------------------	--	--	----------

9 Finance							
	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
9.1	Annual accounts	No	<u>Financial Regulations</u>	Current year + 6 years	Review to see if further retention is needed or SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL
9.2	Loans and grants	No	<u>Financial Regulations</u>	Date of last payment on loan + 12 years	Review to see if further retention is needed or SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL
9.3a	Contracts - under seal	No		Contract completion date + 12 years	SHRED or delete securely		OFFICIAL

9.3b	Contracts - <i>under signature</i>	No		Contract completion date + 6 years	SHRED or delete securely		OFFICIAL
9.3c	Monitoring records	No		Current year + 2 years	SHRED or delete securely		OFFICIAL
9.4	Copy orders	No		Current year + 2 years	SHRED or delete securely		OFFICIAL
9.5	Budget reports, budget monitoring, etc.	No		Current year + 3 years	SHRED or delete securely		OFFICIAL
9.6	Invoice, receipts and other records covered by the Financial regulations	No	<u>Financial Regulations</u>	Current year + 6 years	SHRED or delete securely		OFFICIAL
9.7	Annual budget and background papers	No		Current year + 6 years	SHRED or delete securely		OFFICIAL
9.8	Order books and requisitions	No		Current year + 6 years	SHRED or delete securely		OFFICIAL
9.9	Delivery documentation	No		Current year + 6 years	SHRED or delete securely		OFFICIAL
9.10	Debtors' records	No	<u>Limitation Act 1980</u>	Current year + 6	SHRED or		OFFICIAL

				years	delete securely		
9.11	School fund - <i>Cheque book</i>	No		Current year + 3 years	SHRED or delete securely		OFFICIAL
9.11a	School fund - <i>Paying in books</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.11 b	School fund - <i>Ledger</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.11c	School fund - <i>Invoices</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.11 d	School fund - <i>Receipts</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.11 e	School fund - <i>Bank statements</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.11f	School fund - <i>School journey books</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.12	Free school meals registers	Yes	<u>Financial Regulations</u>	Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE

9.13	Petty case books	No	<u>Financial Regulations</u>	Current year + 6 years	SHRED or delete securely		OFFICIAL
------	------------------	----	------------------------------	------------------------	--------------------------	--	----------

10 Property							
	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
10.1	Title deeds	No		Permanent	These should follow the property, unless the property has been registered at the Land Registry	Consider transferring to <u>Archives</u> , if the deeds are no longer needed	OFFICIAL
10.2	Plans	No		Permanent	Retain in school whilst operational	Consider transferring to <u>Archives</u> , if the plans are no longer needed	OFFICIAL-SENSITIVE
10.3	Maintenance and contractors	No	<u>Financial Regulations</u>	Current year + 6 years	SHRED or delete securely		OFFICIAL
10.4	Leases	No		Expiry of lease + 6 years	SHRED or delete securely		OFFICIAL

10.5	Lettings	No		Current year + 3 years	SHRED or delete securely		OFFICIAL
10.6	Burglary, theft and vandalism report forms	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL
10.7	Maintenance log books	No		Last entry + 10 years	SHRED		OFFICIAL
10.8	Contractors' reports	No		Current year + 6 years	SHRED or delete securely		OFFICIAL

## 11 Local Education Authority

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
11.1	Year 6 admission to independent school confirmation letters	Yes		Current year + 2 years	SHRED or delete securely		OFFICIAL-SENSITIVE
11.2	Attendance returns	Yes		Current year + 1 year	SHRED or delete securely		OFFICIAL-SENSITIVE
11.3	Circulars from LEA	No		Whilst required operationally	Review to see if further retention is needed or SHRED or	Consider transferring to <u>Archives</u>	OFFICIAL



					delete securely		
--	--	--	--	--	-----------------	--	--

## 12 Department for Children, Schools and Families

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
12.1	OFSTED reports and papers	No		Replace former report with any new inspection report	Schools may wish to retain copies for former reports for longer	Consider transferring to <u>Archives</u>	OFFICIAL
12.2	Returns	No		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
12.3	Circulars from Department for Children, Schools and Families	No		Whilst operational required	Review to see if further retention is needed or SHRED	Consider transferring to <u>Archives</u>	OFFICIAL

## 13 Family Support, Liaison and Parent Support

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
13.1	Day books	Yes		Current year + 2 years (then	SHRED or delete		OFFICIAL-SENSITIVE

				review)	securely		
13.2	Reports for outside agencies - <i>where the report has been included on the case file created by the outside agency</i>	Yes		Whilst the child is attending the school then destroy	SHRED or delete securely		OFFICIAL-SENSITIVE
13.3	Referral forms	Yes		Whilst referral is current	SHRED or delete securely		OFFICIAL-SENSITIVE
13.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SHRED or delete securely		OFFICIAL
13.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	SHRED or delete securely		OFFICIAL
13.6	Group registers	Yes		Current year + 2 years	SHRED or delete securely		OFFICIAL
13.7	CAFs	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE

Section 14 relates to Nurseries

## 14 Other Records

### Other Records - Administration FINANCE

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
15.1	Financial records - accounts, statements, invoices, petty cash etc	No		Current year + 6 years	SHRED or delete securely		OFFICIAL

### Other Records - Administration INSURANCE

14.4 b	Insurance policies - Employers Liability	No	<u>Employers Liability</u> <u>Financial Regulations</u>	The policies are kept for a minimum of 6 years and a maximum of 40 years depending on the type of policy	SHRED		OFFICIAL
14.4 c	Claims made against insurance policies - damage to property	Yes		Case concluded + 3 years	SHRED or delete securely		OFFICIAL
14.4 d	Claims made against insurance policies - personal injury	Yes		Case concluded + 6 years	SHRED or delete securely		OFFICIAL

### Other Records - Administration HUMAN RESOURCES

14.5	Personal Files -	Yes		Termination + 6	SHRED or		OFFICIAL-SENSITIVE
------	------------------	-----	--	-----------------	----------	--	--------------------

a	records relating to an individual's employment history			years then review	delete securely		
14.5 b	Pre-employment vetting information (including DBS checks)	Yes	<u>DBA guidelines</u>	Date of check + 6 months	SHRED or delete securely		OFFICIAL-SENSITIVE
14.5 c	Staff training records - general	Yes		Current year + 2 years	SHRED or delete securely		OFFICIAL
14.5 d	Training (proof of completion such as certificates, awards, exam results)	Yes		Last action + 7 years	SHRED or delete securely		OFFICIAL
<b>Other Records - Administration PREMISES AND HEALTH AND SAFETY</b>							
14.5 e	Premises files (relating to maintenance)	No		Cessation of use of building +7 years then review	SHRED		OFFICIAL
14.5 f	Risk Assessments	No		Current year + 3 years	SHRED		OFFICIAL