



# Data Protection Policy



## Bentley CEVC and Copdock Primary Schools Federation

Approved by:	Whole Governing Body	Date: 9/02/22
Last reviewed on:	February 2022	
Next review due by:	Summer Term 2024	

### Contents

1. Aims .....	1
2. Legislation and guidance .....	2
3. Definitions .....	2
4. The data controller .....	3
5. Roles and responsibilities .....	3
6. Data protection principles.....	4
7. Collecting personal data.....	4
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. 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.....	10
18. Monitoring arrangements .....	10
Appendix 1: Personal data breach procedure.....	11

### 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 U.K. data protection law.

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 UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020 and the Data Protection Act 2018 (DPA 2018).

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

It also reflects the ICO's guidance 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
<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, living 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>• 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></ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or</p>

	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 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 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 Tracy Riches and is contactable via [tracey.riches@clear7.co.uk](mailto:tracey.riches@clear7.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 UK
  - 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 UK 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 schools aim 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 or exercise its **official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

## 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 record retention schedule.

## 8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 UK data protection law
  - Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with UK 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

To help individuals exercise this right we provide a form on our website. Hard copies of the form can be requested from the School Office. We ask that Subject Access Requests (SARs) are made using this form so that we can ensure that we provide the information requested. However, SARs can also be made verbally or by letter or email. The SAR should include; the name of the individual, correspondence address, contact number and email address, details of the information requested.

If staff receive an SAR, 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

### 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

## **11. CCTV**

We use CCTV in various locations around the school site (Bentley only), to ensure it remains safe. We will adhere to the ICO's guidance for the use of CCTV and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to Joanne Austin – Headteacher, or Julie Cumberland - Office Manager (Bentley).

## **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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the schools take photographs or videos, 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.

## **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 schools' 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, 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, 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 10 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 and should not use passwords from other sites
- 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 Online Safety, Acceptable Use of ICT and ICT policies).
- 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.

A detailed document retention schedule has been included in Appendix 2 of this policy.

## **16. 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the schools' 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 schools' processes make it necessary.

## **18. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated in the event of any changes to data protection legislation and annually for approval by the full Governing Board.

## **19. Links with other policies**

This policy is linked to our Freedom of information publication scheme, Online Safety Policy, Acceptable Use of ICT Policy, ICT Policy, Child Protection & Safeguarding Policy.

## Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO by email
- 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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered likely that this is the case, 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. Relevant staff members or data processors should help the DPO with this where necessary and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case they are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's secure ICT system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
  - A description, in clear plain language, of the nature of the personal data breach
  - 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 consider, in the light of the investigation and any engagement with affected individuals, whether to 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 secure ICT 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.
- The DPO and Headteacher will meet at least annually to assess recorded data breaches and identify any trends or patterns requiring action by the schools to reduce risks of future breaches

#### Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to 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 endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- If safeguarding information is compromised, the DPO will inform the DSL and discuss whether the school should inform any, or all, of its local safeguarding partners

Other types of breach could include:

- Details of pupil premium interventions for named children being published on the schools' website
- Non-anonymised pupil exam results or staff pay information being shared generally with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- If such a system is in use, the schools' cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families





## Appendix 2 – Information Retention Schedule

### Bentley and Copdock Primary Schools Federation

### Information 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-schools>. 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
2.1	Minutes & Agendas Inspection copies Principal Set (signed)	No  Maybe, if staff-related		Date of meeting + 3 years  <b>Permanent</b>	SHRED or delete securely	Consider transferring to <a href="#">Archives</a>	OFFICIAL
2.2	Agendas (except 1 copy)	No		Date of meeting	SHRED		OFFICIAL
2.3	Reports	Maybe if staff-related		Date of meeting + 6 years unless referred to in Minutes, in which case keep with Principal Set	SHRED	Consider transferring to <a href="#">Archives</a>	OFFICIAL
2.4	Annual parents' meeting papers	No		Date of meeting + 6 years	SHRED	Consider transferring to <a href="#">Archives</a>	OFFICIAL
2.5	Trusts and Endowments	No		Permanent <i>(Retain in school whilst operationally required)</i>	SHRED	Consider transferring to <a href="#">Archives</a>	OFFICIAL
2.6	Action plans created & administered by the GB	No		Until superseded or whilst relevant	SHRED	Consider transferring to <a href="#">Archives</a>	OFFICIAL
2.7	Governor attendance records  Records of governor monitoring minutes  Annual reports to DfE	Yes  Yes  No		Last meeting in the record + 6 years  Visit date + 3 years  Date + 10 years	SHRED		

2.8	Records of election of parent governors Records of co-opted governors Record of election of Chair & Vice-Chair	Yes		Election date +6 months  If decision recorded in Minutes, end of term  Destroy once recorded in Minutes	SHRED		
2.9	Policy documents	No		Until superseded. Retain CP & Safeguarding Policy and pupil-related policies, e.g. exclusions	SHRED	Consider transferring to <u>Archives</u> if part of a past decision making process	OFFICIAL
2.10	Governors' Code of Conduct	No		Permanent copy of each document			
2.11	Complaints files	Yes		Date of resolution of major complaint + 6 years, if negligence + 15 years, CP & Safeguarding issues + 40 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
2.12	Proposals to change the status of the schools to academies	No		Permanent	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
2.13	Correspondence sent / received by GB or HT	Maybe		General – current year + 3			



2.1 4	Records re appointment of Clerk to GB  Records re governors' term of office  Register of business interests  Records of training, records of induction of new governors, governors' personnel files	Yes		End of term + 6 yrs  End of term + 6 yrs  End of term + 6 yrs  End of term + 6 yrs			
----------	---	-----	--	--	--	--	--

### 3 Headteacher & Senior Management Team

	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 of school activity	Yes [1]		Date of last entry in the book + 6 years then review	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 meeting + 5 years	Retain in school for 5 years from date of meeting	Consider transferring to <u>Archives</u>	OFFICIAL
3.3	Reports created by the Headteacher or the Management Team	Yes [1]		Date of report + 3 years	Retain in school for 3 years from date of meeting	Consider transferring to <u>Archives</u>	OFFICIAL
3.4	Records created by Headteacher or other members of staff with administrative responsibilities	Yes [1]		Current academic year + 6 years then review annually	SHRED or delete securely		OFFICIAL

3.5	Correspondence created by Headteacher or other members of staff with administrative responsibilities	No		Date of correspondence + 3 years then review	SHRED or delete securely		OFFICIAL
3.6	Professional development plans	Yes		Add to personnel file or leaving date + 6 years	SHRED or delete securely		OFFICIAL
3.7	School Development Plans	No		Life of Plan + 3 years		Consider transferring to <u>Archives</u>	OFFICIAL
3.8	Admissions Policy – all records re. creation & implementation	No		Policy life + 3 years then review	SHRED		OFFICIAL
3.9	Admissions - <i>Successful</i>	Yes		Date of admission + 1 year	SHRED		OFFICIAL-SENSITIVE
3.10	Admissions - <i>Unsuccessful at appeal</i>	Yes		Date of decision + 1 year	SHRED or delete securely		OFFICIAL-SENSITIVE
3.11	Proof 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.</u>	Date of entry on register + 3 years	Attendance registers are held in hard copy &		OFFICIAL-SENSITIVE

			<u>1751)</u>		electronically on SIMS. The hard copy will be destroyed once the class leaves.		
4.3	Pupil record cards - <i>Primary</i>	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 files - <i>Primary</i>	Yes		Retain for the time which the pupil remains at the primary school  Management information system pupil records 3 years	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
4.5	Special Education Needs files, reviews and Education Health & Care Plans, including advice & information provided to parents regarding educational needs & accessibility strategy	Yes		DOB of the pupil + 31 years (25 + 6)	SHRED or delete securely		OFFICIAL-SENSITIVE
4.6	Correspondence re absence, authorised &	Yes		Current academic year + 2	SHRED or delete securely		OFFICIAL

	unauthorised			years			
4.7	Absence books	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
4.8	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
4.9	Examination results - <i>Internal</i>	Yes		Current year + 5 years	SHRED or delete securely		OFFICIAL
4.1 0	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
4.1 1	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
4.1 2	Proposed statement or amended statement	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
4.1 3	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 4	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 5	Children's SEN files	Yes		Primary schools retain for the time which the pupil remains at the primary school	SHRED or delete securely - unless legal action is pending Pupil file moves onto new school		OFFICIAL-SENSITIVE

4.1 6	Parental permission slips for school trips <i>– where there has been no major incident</i>	Yes		Do RA to assess if required. If not, after trip or end of year	SHRED or delete securely		OFFICIAL-SENSITIVE
4.1 7	Parental permission slips for school trips <i>– where there has been a major incident</i>	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
4.1 8	Records created by schools to obtain approval to run an Educational Visit outside the Classroom <i>- Primary Schools</i>	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
4.1 9	Pupil Premium fund records	Yes		Date of leaving + 6 years			
4.2 0	Dinner Register	Yes		Current year + 3 years	SHRED or delete securely		OFFICIAL
4.2 1	School meals summary sheets	Yes		Current year + 3 years	SHRED or delete securely		OFFICIAL
4.2 2	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 period or SHRED		OFFICIAL
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 period or SHRED		OFFICIAL
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

5.1 1	SATS records (composite)	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
5.1 2	PAN records	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
5.1 3	Value added and contextual data	Yes		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE

## 6 Staff Related

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
6.1	Absence & sickness record, staff returns & timesheets	Yes	<u>Financial regulations</u>	Current year + 3 years Sickness absence with sick pay – current year + 6 years	SHRED or delete securely		OFFICIAL
6.2	Staff personal files	Yes		Termination + 6 years	SHRED or delete securely		OFFICIAL
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months. Successful applicant records go on personnel file	SHRED or delete securely		OFFICIAL
6.4	Pre-employment vetting information (including DBS checks)	Yes	<u>DBS guidelines</u>	Date of check + max 6 months for DBS. If successful, add to file, if not, keep max 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				OFFICIAL-SENSITIVE

			further advice.				
6.6a	Disciplinary proceedings – Warning- <i>oral</i>	Yes		Date of warning + 6 months	SHRED or delete securely		OFFICIAL
6.6b	Disciplinary proceedings – Warning- <i>written (level one)</i>	Yes		Date of warning + 6 months	SHRED or delete securely		OFFICIAL
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 + 6 years	SHRED or delete securely		OFFICIAL
6.8	Salary records	Yes		Current year + 6 years	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 Powers) Regulations 1995</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



## 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.</u> <u>Limitation Act 1980.</u>				
7.2a	Accident reporting- - <i>Adults over 18 (all accidents)</i>	Yes		Last entry in book +3 years Records relating to accident / injury at work + 12 years	SHRED or delete securely		OFFICIAL-SENSITIVE
7.2b	Accident reporting- - <i>Children (all accidents)</i>	Yes		Last entry in book + 3 years	SHRED or delete securely		OFFICIAL-SENSITIVE
7.3	<u>COSHH</u>	No		Date of incident + 40 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	H&S risk assessments	No		Life of RA +3 years. Store with accident report if accident occurs	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		2 years from date examination made. Check for current practice	SHRED		OFFICIAL
7.9	Fire Precautions log books	No		Current year + 3 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 insurance 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>	Maybe		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 & related records	No		Current academic year + 3 years	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL
8.5	Circulars & related records (staff / parents / pupils)	No		Current academic year + 1 year	SHRED		OFFICIAL
8.6	Newsletters, ephemera	No		Current academic year + 1 year	Review to see if further retention is needed - or SHRED	Consider transferring to <u>Archives</u>	OFFICIAL

8.7	Visitors book	Yes		Last entry + 6 years then review	SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL
8.8	Consents re. school activities (GDPR compliance) e.g.to receive circulars, mailings	Yes		When child leaves school			
8.9	Privacy Notice (sent to parents for GDPR compliance)	No		Until superseded + 6 years			
8.10	PTA / Old pupils association records	Yes		Current year + 6 years then review	SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL
8.11	Subject Access Requests	Yes		Data retained for 6 months from date of release  Record of request retained for 2 years			

## 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	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	SHRED or delete securely	Consider transferring to <u>Archives</u>	OFFICIAL
9.3a	Contracts - <i>under seal</i>	No		Last payment + 12 years	SHRED or delete securely		OFFICIAL
9.3b	Contracts - <i>under signature</i>	No		Last payment + 6 years	SHRED or delete securely		OFFICIAL

9.3c	Monitoring records of contracts	No		Life of contract + 6 or 12 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		Life of budget + 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 financial year + 6 years	SHRED or delete securely		OFFICIAL
9.7	Annual budget and background papers	No		Life of budget + 3 years	SHRED or delete securely		OFFICIAL
9.8	Order books and requisitions	No		Current financial 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 years	SHRED or delete securely		OFFICIAL
9.11	School fund - <i>Cheque book</i>	No		Current year + 6 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
9.11b	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
9.1	School fund	No		Current year + 6	SHRED or delete		OFFICIAL

1d	- <i>Receipts</i>			years (the review)	securely		
9.1 1e	School fund - <i>Bank statements</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.1 1f	School fund - <i>School journey books</i>	No		Current year + 6 years (the review)	SHRED or delete securely		OFFICIAL
9.1 2	Free school meals registers where register used as a basis for funding  School Meals Registers & Summary Sheets	Yes	<u>Financial Regulations</u>	Current year + 6 years  Current year + 3 years	SHRED or delete securely		OFFICIAL-SENSITIVE
9.1 3	Petty cash 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> ,	OFFICIAL
10.2	Plans	No		Permanent	Retain in school whilst operational	Consider transferring to <u>Archives</u>	OFFICIAL-SENSITIVE
10.3	Records of maintenance of the school	No	<u>Financial Regulations</u>	Permanent	Follow any transfer of the property		OFFICIAL
10.4	Leases	No		Expiry of lease + 6 years	SHRED or delete securely		OFFICIAL
10.5	Lettings	No		Current year + 6 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		Permanent			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	SHRED or delete	Consider transferring to <u>Archives</u>	OFFICIAL

## 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 to central government	No		Current year + 6 years	SHRED or delete securely		OFFICIAL-SENSITIVE
12.3	Circulars from Department for Children, Schools and Families	No		Operational use	SHRED	Consider transferring to <u>Archives</u>	OFFICIAL

### 13 Family Liaison Officers and Parent Support Assistants

	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 review)	SHRED or delete securely		OFFICIAL-SENSITIVE
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

### 14.1 Early Years Provision (Childcare / Nursery provision, etc.)

Records to be kept by Registered Persons - All Cases

	Basic file description	DP Issues	Statutory provisions	Retention period	Action at end of the administrative life of the record		Protective marking classification
14.1a	Looked After Child (LAC) - <i>contact details, including DOB,</i>	Yes		Closure of setting + 50 years	SHRED or delete	These could be required to show whether or not an individual child	OFFICIAL-SENSITIVE

	<i>of each child who is looked after on the premises</i>				securely	attended the setting in a child protection investigation	
14.1b	Looked After Child (LAC) <i>- contact details of a parent, or person, of each child who is looked after on the premises</i>	Yes		Termination + 6 years then review	SHRED or delete securely		OFFICIAL-SENSITIVE
14.1c	Looked After Child (LAC) <i>- daily record of children looked after on the premises, their hours of attendance and the names of the persons who looked after them</i>	Yes	<u>The Day Care and Child Minding (National Standards) (England) Regulations 2003</u>	Current year + 2 years  Unless likely to be needed in a child protection setting then the records should be retained for closure of setting + 50 years	SHRED or delete securely		OFFICIAL-SENSITIVE
14.1d	A record of accidents occurring on the premises and incident books relating to other incidents	Yes	<u>The Day Care and Child Minding (National Standards) (England) Regulations 2003</u>	DOB of the child involved in the accident or the incident + 25 years  If an adult is injured then the accident book must be kept for 7 years from the date of the incident	SHRED or delete securely		OFFICIAL
14.1e	A record of any medicinal product administered to any child on the premises  (including the date, circumstances of administration, by whom it was administered, medicinal products administered, together with a record of parent's consent)	Yes	<u>The Day Care and Child Minding (National Standards) (England) Regulations 2003</u>	DOB of the child being given/taking the medicine + 25 years	SHRED or delete securely		OFFICIAL-SENSITIVE
14.1f	Records of transfer	Yes		One copy is to be given to the parents, one copy transferred to the Primary			OFFICIAL



				School where the child is going			
14.1g	Portfolio of work, observations and so on	Yes		To be sent home with the child			OFFICIAL
14.1h	Birth certificates	Yes		Once the school has seen the birth certificate and recorded the necessary information, the original can be returned to the parents. There is no requirement to keep a copy of the birth certificate.			OFFICIAL-SENSITIVE

## 15 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 financial year + 6 years	SHRED or delete securely		OFFICIAL

### Other Records – Administration INSURANCE

15.2a	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
15.2b	Claims made against insurance policies – damage to property	Yes		Case concluded + 3 years	SHRED or delete securely		OFFICIAL
15.2c	Claims made against insurance policies – personal injury	Yes		Case concluded + 6 years	SHRED or delete securely		OFFICIAL

### Other Records – Administration HUMAN RESOURCES

15.3a	Personal Files - records relating to an individual's employment history	Yes		Termination + 6 years then review	SHRED or delete securely		OFFICIAL-SENSITIVE
15.3b	Pre-employment vetting information (including DBS checks)	Yes	<u>DBA guidelines</u>	Add to personnel file. DBS - date of check + max. 6 months	SHRED or delete securely		OFFICIAL-SENSITIVE
15.3c	Staff training records – not child-related e.g. first aid, H&S Child-related e.g. SG	Yes		Add to personnel file  Date of training + 40 years	SHRED or delete securely		OFFICIAL
15.3d	Training (proof of completion such as certificates, awards, exam results)  For CPD	Yes		Last action + 7 years  As required by professional body	SHRED or delete securely		OFFICIAL
<b>Other Records – Administration PREMISES AND HEALTH AND SAFETY</b>							
15.3e	Premises files (relating to maintenance)	No		Cessation of use of building +7 years then review	SHRED		OFFICIAL

15.3f	Risk Assessments	No		Current year + 3 years	SHRED		OFFICIAL
-------	------------------	----	--	------------------------	-------	--	----------