

Aylesford School

and Sixth Form College



wonder aspiration respect discipline

DATA PROTECTION POLICY

Written: September 2018
Review Date: October 2020
Lead: HR Officer
Via: Standards, Personnel and Curriculum

'from potential to reality'

Tapping Way, Warwick, Warwickshire, CV34 6XR

Tel: 01926 747100 **Fax:** 01926 494194 **Email:** office@aylesford-elearning.net **Web:** www.aylesfordschool.org.uk

A charitable company registered in England and Wales, company number 7848367

Headteacher: Steven Hall BSc MA

Data Protection Policy

1. Introduction

Aylesford School and Sixth Form College 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 Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Aylesford School and Sixth Form College recognises that by effectively managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

This policy applies to all School Governors and employees, and individuals about whom the school processes personal information, as well as other partners and companies with which the school undertakes its business.

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with the School's funding agreement and articles of association.

2. Scope

Aylesford School and Sixth Form College processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.

Aylesford School and Sixth Form College is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Aylesford School and Sixth Form College needs to collect and use certain types of personal information about people with whom it deals in order to operate. These include current, past and prospective employees, students, suppliers and others with whom it communicates.

In addition, the School may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with correctly, however it is collected, recorded and used.

This policy applies to all records created, received or maintained by staff of Aylesford School and Sixth Form College in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period as defined in Appendix 2) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.

3. Responsibilities

This policy applies to all staff employed Aylesford School and Sixth Form College, and to external organisations, volunteers and other individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 Governing Body

The Governing Body has overall responsibility for ensuring that Aylesford School and Sixth Form College complies with all relevant data protection obligations.

3.2 Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to the School in order to assist the School to implement this policy, monitor compliance with data protection law, and develop related policies and guidelines where applicable.

The DPO will carry out an annual audit of Aylesford School and Sixth Form College data processing activities and report to the Governing Body 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.

Our DPO is the School DPO Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively;

School Data Protection Officer
Warwickshire Legal Services
Warwickshire County Council
Shire Hall
Market Square
Warwick
CV34 4RL

3.3 Head teacher

The Head teacher acts as the representative of the data controller on a day-to-day basis.

3.4 School Business Manager

Aylesford School and Sixth Form College has nominated the following individual as the designated person to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer:

Sue Grinnell, School Business Manager – grinnell.s@aylesford-elearning.net

3.5 All Staff

All members of 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 the School Business Manager 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

4. Data Protection Principles

The GDPR is based on data protection principles that our School must comply with. Aylesford School and Sixth Form College has adopted the principles to underpin its Data Protection Policy:

The principles require that all personal data shall be:

- (1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- (2) used for specified, explicit and legitimate purposes ('purpose limitation');
- (3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');
- (4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');
- (5) kept no longer than is necessary ('storage limitation');
- (6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

This policy sets out how the School aims to comply with these principles.

5. Collecting personal data

5.1 Lawfulness, fairness and transparency

Aylesford School and Sixth Form College shall only process personal data where it has one of 5 'lawful bases' (legal reasons) available to School to do so under data protection law:

- 1) 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
- 2) The data needs to be processed so that the school can comply with a legal obligation
- 3) The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- 4) The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- 5) The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

5.2 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 guidance set out in School's Record Retention Schedule (Appendix 2).

6. Sharing personal data

We will not normally share personal data with anyone else except as set out in the School's Privacy Notice. GDPR and the DPA 2018 also allow information to be shared 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.

7. Subject access requests and other rights of individuals

7.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

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

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

The DPO will send the subject access request to the School Business Manager. If staff receive a subject access request they must immediately forward it to the School Business Manager, who will ensure that the DPO is informed.

Information to be released will be collated by the School and then sent to the DPO for checking and sending out to the applicant.

7.2 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 person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at our school aged 13 and above may not be granted without the express permission of the pupil.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at our school [aged under 13] will in general be granted without requiring the express permission of the pupil.

These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

7.3 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, or where it is impractical to comply within a month due to school closure. 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.

7.4 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 5), individuals also have the right to:

- Withdraw their consent to processing at any time, where processing is based on the consent of the pupil or parent
- 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 School Business Manager who will send it to the DPO for information purposes.

8. Biometric recognition systems

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

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

Parents/carers and pupils have the right to choose not to use the School's biometric systems. We will provide alternative means of accessing the relevant services for those pupils.

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

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

9. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to Sue Grinnell, School Business Manager.

10. Photographs and videos

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

Aylesford School and Sixth Form College will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials – in the Home School Agreement. We will clearly explain how the photograph and/or video will be used to both the parent/carers and pupil.

Where the School need parental consent, it shall clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where the School don't need parental consent, it shall clearly explain to the pupil how the photograph and/or video will be used.

All schools add and adapt to reflect your school's uses of photographs and videos for communication, marketing and promotional materials:

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.

11. Data protection by design and default

Aylesford School and Sixth Form College shall put measures in place to show that it has integrated data protection into all of its 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 4)
- 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
- 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

12. Data security and storage of records

Aylesford School and Sixth Form College 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
- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it.
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, 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 the Information Security Policy on acceptable use)
- 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 6)

13. 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, the School will shred 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.

14. Personal data breaches

Aylesford School and Sixth Form College shall take all reasonable steps 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, the School shall 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

15. 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.

16. Links with other policies

This data protection policy is linked to our:

Information Security Policy

Security Incidents and Business Continuity Policy

E-Safety Policy

Appendix 1: Personal data breach procedures

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

When appropriate, the School will report the data breach to the ICO within 72 hours in accordance with the requirements of the GDPR.

1. Data protection breaches occur where personal data is lost, damaged, destroyed, stolen, misused and/or accessed unlawfully.
2. Examples of how a breach may occur include:
 - a. Theft of data or equipment on which data is stored;
 - b. Loss of data or equipment on which data is stored;
 - c. Inappropriate access controls allowing unauthorised use;
 - d. Accidental Loss;
 - e. Destruction of personal data;
 - f. Damage to personal data;
 - g. Equipment failure;
 - h. Unlawful disclosure of personal data to a third party;
 - i. Human error;
 - j. Unforeseen circumstances such as fire or flood;
 - k. Hacking attack; or
 - l. 'Blagging' offences where information is obtained by deceiving the organisation which holds it.
3. If any member of staff of Aylesford School and Sixth Form College or Governor discovers that data has been lost, or believes that there has been a breach of the data protection principles in the way that data is handled, you must immediately or no later than within 24 hours of first coming to notice, inform the School Business Manager.
4. Upon being notified, the School Business Manager will assess whether a breach of personal information has occurred, and the level of severity. If a breach has occurred but the risk of harm to any individual is low (for example, because no personal information has left the control of the School, then the **School Business Manager** will undertake an internal investigation to consider whether the Information Security Policy was followed, and whether any alterations need to be made to internal procedures as a result.
5. In all other cases, the incident must be notified to the Data Protection Officer immediately, who must follow the Information Commissioner's Office guidelines on notification and recording of the breach. The priority must then be to close or contain the breach to mitigate / minimise the risks to those individuals affected by it.

All Aylesford School staff and Governors are expected to work in partnership with the School Business Manager and the Data Protection Officer in relation to the following matters

Notification of Breaches

Any member of staff or Governor who becomes aware of a personal information breach should provide full details to the School Business Manager within 24 hours of being made aware of the

breach. The School Business Manager will then complete the Data Breach Record Form and Incident Log. When completing the form details should be provided of the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type of breach and information about personal data concerned. Details of what has already been done to respond to the risks posed by the breach should also be included.

Containment and Recovery

The initial response is to investigate and contain the situation and a recovery plan including, damage limitation. You may need input from specialists such as IT, HR and legal and in some cases contact with external third parties.

- Seek assistance in the containment exercise. This could be isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Consider whether any individual affected by the data breach should be notified

Assessing the Risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. For example, if a case file is lost then risks are different depending on type of data and its sensitivity with potential adverse consequences for individuals. The School Business Manager should consider the following points:

- What type of data is involved?
- How sensitive is the data?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?
- If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk.
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data has been affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to life?
- Loss of public confidence in the School?

All staff and Governors should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Appendix 2 – Record Retentions

1. Management of the School

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

| 1.1 Governing Body | | | | | |
|--------------------|--|--|---|---|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 1.1.1 | Agendas for Governing Body meetings | There may be data protection issues if the meeting is dealing with confidential issues relating to staff | One copy should be retained with the master set of minutes. All other copies can be disposed of | SECURE DISPOSAL ¹ | |
| 1.1.2 | Minutes of Governing Body meetings | There may be data protection issues if the meeting is dealing with confidential issues relating to staff | | | |
| | Principal Set (signed) | | PERMANENT | If the school is unable to store these then they should be offered to the County Archives Service | |
| | Inspection Copies ² | | Date of meeting + 3 years | If these minutes contain any sensitive, personal information they must be shredded. | |
| 1.1.3 | Reports presented to the Governing Body | There may be data protection issues if the report deals with confidential issues relating to staff | Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently | SECURE DISPOSAL or retain with the signed set of the minutes | |
| 1.1.4 | Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002 | No | Date of the meeting + a minimum of 6 years | SECURE DISPOSAL | |

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

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

| 1.1 Governing Body (continued...) | | | | | |
|--|---|-------------------------------|--|--|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 1.1.5 | Instruments of Government including Articles of Association | No | PERMANENT | These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes. | |
| 1.1.6 | Trusts and Endowments managed by the Governing Body | No | PERMANENT | These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes. | |
| 1.1.7 | Action plans created and administered by the Governing Body | No | Life of the action plan + 3 years | SECURE DISPOSAL | |
| 1.1.8 | Policy documents created and administered by the Governing Body | No | Life of the policy + 3 years | SECURE DISPOSAL | |
| 1.1.9 | Records relating to complaints dealt with by the Governing Body | Yes | Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes | SECURE DISPOSAL | |
| 1.1.10 | Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 | No | Date of report + 10 years | SECURE DISPOSAL | |
| 1.1.11 | Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies | No | Date proposal accepted or declined + 3 years | SECURE DISPOSAL | |

| 1.2 Head Teacher and Senior Management Team | | | | | |
|--|--|---|---|--|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 1.2.1 | Log books of activity in the school maintained by the Head Teacher | There may be data protection issues if the log book refers to individual pupils or members of staff | Date of last entry in the book + a minimum of 6 years then review | These could be of permanent historical value and should be offered to the County Archives Service if appropriate | |
| 1.2.2 | Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies | There may be data protection issues if the minutes refers to individual pupils or members of staff | Date of the meeting + 3 years then review | SECURE DISPOSAL | |
| 1.2.3 | Reports created by the Head Teacher or the Management Team | There may be data protection issues if the report refers to individual pupils or members of staff | Date of the report + a minimum of 3 years then review | SECURE DISPOSAL | |
| 1.2.4 | Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | There may be data protection issues if the records refer to individual pupils or members of staff | Current academic year + 6 years then review | SECURE DISPOSAL | |
| 1.2.5 | Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities | There may be data protection issues if the correspondence refers to individual pupils or members of staff | Date of correspondence + 3 years then review | SECURE DISPOSAL | |
| 1.2.6 | Professional Development Plans | Yes | Life of the plan + 6 years | SECURE DISPOSAL | |
| 1.2.7 | School Development Plans | No | Life of the plan + 3 years | SECURE DISPOSAL | |

| 1.3 Admissions Process | | | | | |
|-------------------------------|--|-------------------------------|--|--|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 1.3.1 | All records relating to the creation and implementation of the School Admissions' Policy | No | Life of the policy + 3 years then review | SECURE DISPOSAL | |
| 1.3.2 | Admissions – if the admission is successful | Yes | Date of admission + 1 year | SECURE DISPOSAL | |
| 1.3.3 | Admissions – if the appeal is unsuccessful | Yes | Resolution of case + 1 year | SECURE DISPOSAL | |
| 1.3.4 | Register of Admissions | Yes | Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made. ³ | REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school. | |
| 1.3.5 | Admissions – Secondary Schools – Casual | Yes | Current year + 1 year | SECURE DISPOSAL | |
| 1.3.6 | Proofs of address supplied by parents as part of the admissions process | Yes | Current year + 1 year | SECURE DISPOSAL | |
| 1.3.7 | Supplementary Information form including additional information such as religion, medical conditions etc | Yes | | | |
| | For successful admissions | | This information should be added to the pupil file | SECURE DISPOSAL | |
| | For unsuccessful admissions | | Until appeals process completed | SECURE DISPOSAL | |

| 1.4 Operational Administration | | | | | |
|---------------------------------------|---|-------------------------------|---------------------------------------|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 1.4.1 | General file series | No | Current year + 5 years then REVIEW | SECURE DISPOSAL | |
| 1.4.2 | Records relating to the creation and publication of the school brochure or prospectus | No | Current year + 3 years | STANDARD DISPOSAL | |
| 1.4.3 | Records relating to the creation and distribution of circulars to staff, parents or pupils | No | Current year + 1 year | STANDARD DISPOSAL | |
| 1.4.4 | Newsletters and other items with a short operational use | No | Current year + 1 year | STANDARD DISPOSAL | |
| 1.4.5 | Visitors' Books and Signing in Sheets | Yes | Current year + 6 years then REVIEW | SECURE DISPOSAL | |
| 1.4.6 | Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations | No | Current year + 6 years then REVIEW | SECURE DISPOSAL | |

2. Human Resources

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

| 2.1 Recruitment | | | | | |
|------------------------|--|-------------------------------|---|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 2.1.1 | All records leading up to the appointment of a new headteacher | Yes | Date of appointment + 6 years | SECURE DISPOSAL | |
| 2.1.2 | All records leading up to the appointment of a new member of staff – unsuccessful candidates | Yes | Date of appointment of successful candidate + 6 months | SECURE DISPOSAL | |
| 2.1.3 | All records leading up to the appointment of a new member of staff – successful candidate | Yes | All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months | SECURE DISPOSAL | |
| 2.1.4 | Pre-employment vetting information – DBS Checks | No | The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months | | |
| 2.1.5 | Proofs of identity collected as part of the process of checking “portable” enhanced DBS disclosure | Yes | Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staff’s personal file | | |
| 2.1.6 | Pre-employment vetting information – Evidence proving the right to work in the United Kingdom ⁴ | Yes | Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years | | |

| 2.2 Operational Staff Management | | | | | |
|---|--------------------------------------|------------------------|-------------------------------------|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 2.2.1 | Staff Personal File | Yes | Termination of Employment + 6 years | SECURE DISPOSAL | |
| 2.2.2 | Timesheets | Yes | Current year + 6 years | SECURE DISPOSAL | |
| 2.2.3 | Annual appraisal/ assessment records | Yes | Current year + 5 years | SECURE DISPOSAL | |

| 2.3 Management of Disciplinary and Grievance Processes | | | | | |
|---|--|------------------------|--|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 2.3.1 | Allegation of a child protection nature against a member of staff including where the allegation is unfounded ⁵ | Yes | Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned | SECURE DISPOSAL These records must be shredded | |
| 2.3.2 | Disciplinary Proceedings | Yes | | | |
| | oral warning | | Date of warning + 6 months | SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file] | |
| | written warning – level 1 | | Date of warning + 6 months | | |
| | written warning – level 2 | | Date of warning + 12 months | | |
| | final warning | | Date of warning + 18 months | | |
| | case not found | | If the incident is child protection related then see above otherwise dispose of at the conclusion of the case | SECURE DISPOSAL | |

| 2.4 Health and Safety | | | | | |
|------------------------------|--|-------------------------------|--|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 2.4.1 | Health and Safety Policy Statements | No | Life of policy + 3 years | SECURE DISPOSAL | |
| 2.4.2 | Health and Safety Risk Assessments | No | Life of risk assessment + 3 years | SECURE DISPOSAL | |
| 2.4.3 | Records relating to accident/ injury at work | Yes | Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied | SECURE DISPOSAL | |
| 2.4.4 | Accident Reporting | Yes | | | |
| | Adults | | Date of the incident + 6 years | SECURE DISPOSAL | |
| | Children | | DOB of the child + 25 years | SECURE DISPOSAL | |
| 2.4.5 | Control of Substances Hazardous to Health (COSHH) | No | Current year + 40 years | SECURE DISPOSAL | |
| 2.4.6 | Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos | No | Last action + 40 years | SECURE DISPOSAL | |
| 2.4.7 | Process of monitoring of areas where employees and persons are likely to have become in contact with radiation | No | Last action + 50 years | SECURE DISPOSAL | |
| 2.4.8 | Fire Precautions log books | No | Current year + 6 years | SECURE DISPOSAL | |

| 2.4 Payroll and Pensions | | | | | |
|---------------------------------|--|-------------------------------|---------------------------------------|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 2.5.1 | Maternity pay records | Yes | Current year + 3 years | SECURE DISPOSAL | |
| 2.5.2 | Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995 | Yes | Current year + 6 years | SECURE DISPOSAL | |

3. Financial Management of the School

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

| 3.1 Risk Management and Insurance | | | | | |
|--|--|------------------------|----------------------------------|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 3.1.1 | Employer's Liability Insurance Certificate | No | Closure of the school + 40 years | SECURE DISPOSAL | |

| 3.2 Asset Management | | | | | |
|-----------------------------|--|------------------------|--------------------------------|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 3.2.1 | Inventories of furniture and equipment | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.2.2 | Burglary, theft and vandalism report forms | No | Current year + 6 years | SECURE DISPOSAL | |

| 3.3 Accounts and Statements including Budget Management | | | | | |
|--|--|------------------------|---|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 3.3.1 | Annual Accounts | No | Current year + 6 years | STANDARD DISPOSAL | |
| 3.3.2 | Loans and grants managed by the school | No | Date of last payment on the loan + 12 years then REVIEW | SECURE DISPOSAL | |
| 3.3.3 | Student Grant applications | Yes | Current year + 3 years | SECURE DISPOSAL | |
| 3.3.4 | All records relating to the creation and management of budgets including the Annual Budget statement and background papers | No | Life of the budget + 3 years | SECURE DISPOSAL | |
| 3.3.5 | Invoices, receipts, order books and requisitions, delivery notices | No | Current financial year + 6 years | SECURE DISPOSAL | |
| 3.3.6 | Records relating to the collection and banking of monies | No | Current financial year + 6 years | SECURE DISPOSAL | |
| 3.3.7 | Records relating to the identification and collection of debt | No | Current financial year + 6 years | SECURE DISPOSAL | |

| 3.4 Contract Management | | | | | |
|--------------------------------|---|-------------------------------|---|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 3.4.1 | All records relating to the management of contracts under seal | No | Last payment on the contract + 12 years | SECURE DISPOSAL | |
| 3.4.2 | All records relating to the management of contracts under signature | No | Last payment on the contract + 6 years | SECURE DISPOSAL | |
| 3.4.3 | Records relating to the monitoring of contracts | No | Current year + 2 years | SECURE DISPOSAL | |

| 3.5 School Fund | | | | | |
|------------------------|-------------------------------|-------------------------------|---------------------------------------|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 3.5.1 | School Fund - Cheque books | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.5.2 | School Fund - Paying in books | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.5.3 | School Fund – Ledger | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.5.4 | School Fund – Invoices | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.5.5 | School Fund – Receipts | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.5.6 | School Fund - Bank statements | No | Current year + 6 years | SECURE DISPOSAL | |
| 3.5.7 | School Fund – Journey Books | No | Current year + 6 years | SECURE DISPOSAL | |

| 3.6 School Meals | | | | | |
|-------------------------|-------------------------------|-------------------------------|---------------------------------------|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 3.6.1 | Free School Meals Registers | Yes | Current year + 6 years | SECURE DISPOSAL | |
| 3.6.2 | School Meals Registers | Yes | Current year + 3 years | SECURE DISPOSAL | |
| 3.6.3 | School Meals Summary Sheets | No | Current year + 3 years | SECURE DISPOSAL | |

4. Property Management

This section covers the management of buildings and property.

| 4.1 Property Management | | | | | |
|-------------------------|--|------------------------|--|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 4.1.1 | Title deeds of properties belonging to the school | No | PERMANENT These should follow the property unless the property has been registered with the Land Registry | | |
| 4.1.2 | Plans of property belong to the school | No | These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold. | | |
| 4.1.3 | Leases of property leased by or to the school | No | Expiry of lease + 6 years | SECURE DISPOSAL | |
| 4.1.4 | Records relating to the letting of school premises | No | Current financial year + 6 years | SECURE DISPOSAL | |

| 4.2 Maintenance | | | | | |
|-----------------|---|------------------------|--------------------------------|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 4.2.1 | All records relating to the maintenance of the school carried out by contractors | No | Current year + 6 years | SECURE DISPOSAL | |
| 4.2.2 | All records relating to the maintenance of the school carried out by school employees including maintenance log books | No | Current year + 6 years | SECURE DISPOSAL | |

5. Pupil Management

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

| 5.1 Pupil's Educational Record | | | | | |
|--------------------------------|---|------------------------|--|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 5.1.1 | Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005 | Yes | | | |
| | Primary | | Retain whilst the child remains at the primary school | The file should follow the pupil when he/she leaves the primary school. ³ | |
| | Secondary | | Date of Birth of the pupil + 25 years | SECURE DISPOSAL | |
| 5.1.2 | Examination Results – Pupil Copies | Yes | | | |
| | Public | | This information should be added to the pupil file | All uncollected certificates should be returned to the examination board. | |
| | Internal | | This information should be added to the pupil file | | |
| 5.1.3 | Child Protection information held on pupil file | | If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file. | SECURE DISPOSAL – these records MUST be shredded | |
| 5.1.4 | Child protection information held in separate files | | DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record | SECURE DISPOSAL – these records MUST be shredded | |

³ This will include: (i) to another primary school (ii) to a secondary school (iii) to a pupil referral unit (iv) If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority

| 5.2 Attendance | | | | | |
|-----------------------|---|-------------------------------|--|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 5.2.1 | Attendance Registers | Yes | Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made. | SECURE DISPOSAL | |
| 5.2.2 | Correspondence relating to authorized absence | | Current academic year + 2 years | SECURE DISPOSAL | |

| 5.3 Special Educational Needs | | | | | |
|--------------------------------------|---|-------------------------------|---|--|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 5.3.1 | Special Educational Needs files, reviews and Individual Education Plans | Yes | Date of Birth of the pupil + 25 years | REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented. | |
| 5.3.2 | Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement | Yes | Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] | SECURE DISPOSAL unless the document is subject to a legal hold | |
| | | | Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] | SECURE DISPOSAL unless the document is subject to a legal hold | |
| | | | Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] | SECURE DISPOSAL unless the document is subject to a legal hold | |

6. Curriculum Management

| 6.1 Statistics and Management Information | | | | | |
|---|--|------------------------|---|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 6.1.1 | Curriculum returns | No | Current year + 3 years | SECURE DISPOSAL | |
| 6.1.2 | Examination Results (Schools Copy) | Yes | Current year + 6 years | SECURE DISPOSAL | |
| | SATS records – | Yes | | | |
| | Results | | The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison | SECURE DISPOSAL | |
| | Examination Papers | | The examination papers should be kept until any appeals/validation process is complete | SECURE DISPOSAL | |
| 6.1.3 | Published Admission Number (PAN) Reports | Yes | Current year + 6 years | SECURE DISPOSAL | |
| 6.1.4 | Value Added and Contextual Data | Yes | Current year + 6 years | SECURE DISPOSAL | |
| 6.1.5 | Self-Evaluation Forms | Yes | Current year + 6 years | SECURE DISPOSAL | |

| 6.2 Implementation of Curriculum | | | | | |
|----------------------------------|------------------------|------------------------|---|---|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 6.2.1 | Schemes of Work | No | Current year + 1 year | Review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL | |
| 6.2.2 | Timetable | No | Current year + 1 year | | |
| 6.2.3 | Class Record Books | No | Current year + 1 year | | |
| 6.2.4 | Mark Books | No | Current year + 1 year | | |
| 6.2.5 | Record homework set | No | Current year + 1 year | | |
| 6.2.6 | Pupils' Work | No | Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year+1 year | SECURE DISPOSAL | |

7. Extra Curriculum Management

| 7.1 Educational Visits outside the Classroom | | | | | |
|--|---|------------------------|---|---|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (v) |
| 7.1.1 | Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools | No | Date of visit + 14 years | SECURE DISPOSAL | |
| 7.1.2 | Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools | No | Date of visit + 10 years | SECURE DISPOSAL | |
| 7.1.3 | Parental consent forms for school trips where there has been no major incident | Yes | Conclusion of the trip | Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time. | |
| 7.1.4 | Parental permission slips for school trips – where there has been a major incident | Yes | DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils | | |

| 7.2 Walking Bus | | | | | |
|-----------------|------------------------|------------------------|--|---|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (v) |
| 7.2.1 | Walking Bus Registers | Yes | Date of register + 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting | SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time] | |

| 7.3 Family Liaison Officers and Home School Liaison Assistants | | | | | |
|---|--|-------------------------------|---|---|---|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 7.3.1 | Day Books | Yes | Current year + 2 years then review | | |
| 7.3.2 | Reports for outside agencies - where the report has been included on the case file created by the outside agency | Yes | Whilst child is attending school and then destroy | | |
| 7.3.3 | Referral forms | Yes | While the referral is current | | |
| 7.3.4 | Contact data sheets | Yes | Current year then review, if contact is no longer active then destroy | | |
| 7.3.5 | Contact database entries | Yes | Current year then review, if contact is no longer active then destroy | | |
| 7.3.6 | Group Registers | Yes | Current year + 2 years | | |

8. Central Government and Local Authority

| 8.1 Local Authority | | | | | |
|---------------------|---|------------------------|--------------------------------|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 8.1.1 | Secondary Transfer Sheets (Primary) | Yes | Current year + 2 years | SECURE DISPOSAL | |
| 8.1.2 | Attendance Returns | Yes | Current year + 1 year | SECURE DISPOSAL | |
| 8.1.3 | School Census Returns | No | Current year + 5 years | SECURE DISPOSAL | |
| 8.1.4 | Circulars and other information sent from the Local Authority | No | Operational use | SECURE DISPOSAL | |

| 8.2 Central Government | | | | | |
|------------------------|--|------------------------|--------------------------------|--|----------------------------------|
| Ref | Basic file description | Data Protection Issues | Retention Period [Operational] | Action at the end of the administrative life of the record | Annual Review Completed Tick (✓) |
| 8.2.1 | OFSTED reports and papers | No | Life of the report then REVIEW | SECURE DISPOSAL | |
| 8.2.2 | Returns made to central government | No | Current year + 6 years | SECURE DISPOSAL | |
| 8.2.3 | Circulars and other information sent from central government | No | Operational use | SECURE DISPOSAL | |