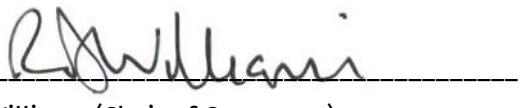
AYLESBURY GRAMMAR SCHOOL

Founded 1598

DATA PROTECTION POLICY

This policy is updated and approved by the Governing Body annually

This version was approved December 2021

SIGNED: 

Richard Williams (Chair of Governors)

AYLESBURY GRAMMAR SCHOOL
Founded 1598

DATA PROTECTION POLICY

1. Introduction & Aims

1.1 The school aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK Data Protection law.

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

2. Legislation and guidance

2.1 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
- Data Protection Act 2018 (DPA 2018)

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

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

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

2.5 In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's:

	• Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

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

4.2 The school is registered as a data controller with the ICO and paid its data protection fee and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

Governing Body

5.2 The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

Data Protection Officer and Data Protection Lead Officer

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

5.4 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.

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

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

5.7 Our DPO and DPLO are contactable via the school address/telephone or by email dpo@ags.bucks.sch.uk

Headmaster

5.8 The headmaster acts as the representative of the data controller on a day-to-day basis.

All staff

5.9 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 DPLO 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

6.1 The UK GDPR is based on data protection principles that our school must comply with.

6.2 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

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

7. Collecting personal data

Lawfulness, fairness and transparency

7.1 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 or another person i.e. 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, 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 student) has freely given clear **consent**

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

- 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

7.3 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

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

7.5 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.

Limitation, minimisation and accuracy

7.6 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.

7.7 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.

7.8 Staff must only process personal data where it is necessary in order to do their jobs.

7.9 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 records management procedure (Appendix 2).

7.10 We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

8. Sharing personal data

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

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies, public authorities and Government bodies
- Our suppliers or contractors need data to enable us to provide services to our staff and students – 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 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

8.2 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

8.3 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 students or staff.

8.4 Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals

Subject access requests

9.1 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

9.2 Subject access requests can be submitted in any form to the DPO. We may be able to respond to requests more quickly if they are made in writing and they should include:

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

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

Children and subject access requests

9.4 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.

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

Responding to subject access requests

9.6 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

9.7 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 student 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
- 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

9.8 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.

9.9 A request may be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

9.10 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.

Other data protection rights of the individual

9.11 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 if the processing relies on consent
- 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

- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Object to decisions based solely on automated decision making or profiling (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)

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

10. Biometric recognition systems

10.1 *Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.*

10.2 Where we use students' biometric data as part of an automated biometric recognition system (for example, students 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.

10.3 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.

10.4 Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can be identified without finger print to charge school dinners to parent pay system if they wish.

10.5 Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

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

11. CCTV

11.1 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 and our CCTV procedure (see Appendix 3)

11.2 The school uses CCTV equipment to provide a safer, more secure environment for students and staff and to prevent anti-social behaviour, bullying, vandalism and theft. Essentially, it is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public, student and staff safety.
- Monitoring the security of the site.

11.3 The school does not use the CCTV system for covert monitoring.

11.3 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.

11.4 Any enquiries about the CCTV system should be directed to the school's DPLO.

12. Photographs and videos

12.1 Photos of Governors, staff and students are used legitimately for security and ID purposes.

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

12.3 We will obtain written consent from parents/carers, or students aged 12 and over if regarded to be mature enough to understand their rights and the implications, for photographs and videos to be taken of students for communication, marketing and promotional materials.

12.4 Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

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

12.5 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.

12.6 When using photographs and videos in this way we will not accompany them with any other personal information about the student, to ensure they cannot be identified unless they consent to this.

12.7 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 ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

13. Data protection by design and default

13.1 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/DPLO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO/DPLO 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 will 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure

14. Data security and storage of records

14.1 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 secure 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 sensitive 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 students are reminded to change their passwords at regular intervals and that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students 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 ICT Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

15.1 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.

15.2 We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Records Management Policy

16.1 The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective 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.

16.2 It covers:

- Scope
- Responsibilities
- Retention and Disposal of records
- Relationships with existing policies

16.3 This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

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

16.5 The policy sets out the approach to be adopted for the retention and disposal of paper and electronic records held in the school, taking into account of legal requirements and good practice depending on the contents of the record.

16.6 A Schedule of Retention (Appendix 2 of this policy) refers to record series regardless of the media in which they are stored.

16.7 A small percentage of the school's records will be selected for permanent preservation as part of the institution's archives and for historical research. This should be done in liaison with the County Archives Service.

16.8 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this process is the Headmaster.

16.9 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

16.10 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

16.11 Under the Freedom of Information Act 2000, schools are required to maintain a retention schedule listing the record series that the school creates in the course of its business.

16.12 The retention schedule lays down the length of time which the record needs to be retained and the action that should be taken when it is of no further administrative use.

16.13 The retention schedule lays down the basis for "normal processing" under both the Data Protection Act 2018/General Data Protection Regulations (UK GDPR) and the Freedom of Information Act 2000.

16.14 The records will be disposed of within 6 months after the retention period indicated in the schedule.

16.15 The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction. Members of staff should record at least:

- File reference (or other unique identifier);
- File title (or brief description);
- Number of files and date range
- The name of the authorising officer
- Date action taken

16.16 If indicated, the file will be securely disposed of in relation to the media it is stored on. If paper this would be shredded (to a minimum of P3 level or equivalent) and other media to a level available with current technology.

16.17 Not withstanding the timescale in the Retention Schedule, data may be disposed of earlier due to a request from a Data subject under Data Protection law if legally obliged to do so.

16.18 If a request of information under Freedom of Information or Data Protection law is received or a legal hold imposed then records disposal relating to the request or legal hold will be stopped whilst the request or hold is operative.

16.19 Managing record series using these retention schedule will be deemed to be "normal processing" under the legislation mentioned above. If record series are to be kept for longer or shorter periods than laid out in this document the reasons for this need to be documented.

17. Personal data breaches

17.1 The school will make all reasonable endeavors to ensure that there are no personal data breaches.

17.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

17.3 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 school website which shows the exam results of students 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 students

18. Training

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

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

19. Monitoring arrangements

19.1 The DPO/DPLO is responsible for monitoring and reviewing this policy.

20. Links with other policies

20.1 This data protection policy is linked to our:

- Freedom of information publication scheme
- Acceptable use of ICT Policy

21. Policy Review

21.1 This policy will be reviewed by the governing body of the school annually.

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

  If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned

    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description, in clear and plain language, of the nature of the personal data breach
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
    - A record of all breaches will be maintained.
- The DPO, DPLO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Appendix 2: Records Management Procedure

Using the Retention Schedule

The Retention Schedule is divided into eight sections:

1. Management of the School
2. Human Resources
3. Financial Management of the School
4. Property Management
5. Pupil Management
6. Curriculum Management
7. Extra-Curricular Activities
8. Central Government and Local Authority

There are sub headings under each section to help guide you to the retention period you are looking for. Each entry has a unique reference number.

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 Headteacher and the senior management team, the admissions process and operational administration.

1.1 Governing Body					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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
1.1.2	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	
	Inspection Copies			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	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
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 + 6 years (major); 15 years (negligence); 40 years (safeguarding or child protection)	SECURE DISPOSAL
1.1.10	Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	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
1.1.12	Records relating to the election of parent and staff governors not appointed by governors	Yes		Date of election + 6 months	SECURE DISPOSAL
1.1.13	Records relating to the appointment of co-opted governors	Yes		Provided decision is in minutes, end of term of office unless allegations concerning children, 25 year	SECURE DISPOSAL
1.1.14	Register of attendance	Yes		Data of meeting + 6 years	SECURE DISPOSAL

1.1.15	Records relating to Governor Monitoring Visits	Yes		Date of visit + 3 years	SECURE DISPOSAL
1.1.16	Records relating to appointment of Clerk	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL
1.1.17	Records relating to terms of office and governor appointments	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL
1.1.18	Records relating to governor declaration against disqualification criteria	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL
1.1.19	Register of business interest	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL
1.1.20	Records relating to training required/received by Governors	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL
1.1.21	Records relating to the induction of new governors	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL
1.1.22	Records of DBS checks on Clerk and members of governing body	Yes		Date of check + 6 months	SECURE DISPOSAL
1.1.23	Governors personnel file	Yes		Appointment ceasing + 6 years	SECURE DISPOSAL

1.2 Headmaster and SLT					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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	SECURE DISPOSAL
1.2.2	Minutes of SLT 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		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL

		individual pupils or members of staff			
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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
1.3.1	All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2	Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Date of admission + 1 year	SECURE DISPOSAL
1.3.3	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for	Resolution of case + 1 year	SECURE DISPOSAL

			admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014		
1.3.4	Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.	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	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period

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 Alumni	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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
2.1.1	All records leading up to the appointment of a new headmaster	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 2.2.1) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4	Pre-employment vetting information – DBS Checks	Yes	DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5	Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure	Yes		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep a copy documentation then this should be placed on the member of staff's personal file	
2.1.6	Pre-employment vetting information – Evidence proving	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File	

	the right to work in the United Kingdom			[see 2.2.1], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	

2.2 Operational Staff Management					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
2.2.1	Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2	Sickness absence monitoring	Yes – Sensitive data		Sick pay not paid – current year + 3 years Sick pay paid - Current year + 6 years	SECURE DISPOSAL
2.2.3	Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL
2.2.4	Staff training – where training leads to continuing professional development	Yes		Length of time required by professional body	SECURE DISPOSAL
2.2.5	Staff training – except where dealing with children (eg first aid or H&S)	Yes		Retained in personnel file (see 2.2.1 above)	SECURE DISPOSAL
2.2.6	Staff training – where training relates to children (eg safeguarding or other child related training)	Yes		Date of training + 40 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
2.3.1	Allegation of a child protection nature against a member of	Yes	"Keeping children safe in education Statutory guidance for schools and	In personnel file until the person's normal retirement age or 10 years from the	SECURE DISPOSAL These records must be shredded

	staff including where the allegation is unfounded		colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files.	
2.3.2	Disciplinary Proceedings	Yes			
	oral warning			Date of warning + 6 months	SECURE DISPOSAL [If 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 2.3.1 otherwise dispose of at the conclusion of the case	SECURE DISPOSAL

2.4 Health and Safety					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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 provided that a copy of the risk assessment is with the accident report if an incident has occurred	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	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration		

			Act 1992 Section 8. Limitation Act 1980		
	Adults			Date of the incident + 6 years	SECURE DISPOSAL
	Children			DOB of the child + 25 years	SECURE DISPOSAL
2.4.5	Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR)	Yes	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 No 1471 Regulation 12(2)	Date of incident + 3 years provided that all records relating to the incident are held on personnel file (see 2.4.2 above)	SECURE DISPOSAL
2.4.6	Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.8	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
2.4.9	Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL

2.5 Payroll and Pensions					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
2.5.1	Absence record	Yes		Current year + 3 years	SECURE DISPOSAL
2.5.2	Car mileage output	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL

2.5.3	Income tax form P60	Yes		Current year + 6 years	SECURE DISPOSAL
2.5.4	Insurance	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.5	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.6	National Insurance – schedule of payments	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.7	Overtime	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.8	Payroll awards	Yes		Current year + 6 years	SECURE DISPOSAL
2.5.9	Payroll – gross/net weekly or monthly	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.10	Payroll reports	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.11	Payslips – copies	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.12	Personal bank details	Yes		Until superseded + 3 years Employment ends + 6 years	SECURE DISPOSAL
2.5.13	Sickness record	Yes		Current year + 3 years	SECURE DISPOSAL
2.5.14	Superannuation adjustments	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.15	Superannuation reports	Yes	Taxes Management Act 1970, Income and Corporation Taxes 1988	Current year + 6 years	SECURE DISPOSAL
2.5.16	Tax forms P6, P11, P11D, P35, P45, P46, P48	Yes		Current year + 6 years	SECURE DISPOSAL
2.5.17	Timesheets/flexitime	Yes		Current year + 3 years	SECURE DISPOSAL

2.5.18	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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
3.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL

3.2 Asset Management					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
3.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL

3.3 Accounts and Statements including Budget Management					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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	Pupil Premium Fund records	Yes		Date student leaves provision + 6 years	SECURE DISPOSAL
3.3.5	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
3.3.6	Invoices, receipts, order books and requisitions, delivery notices		No	Current financial year + 6 years	SECURE DISPOSAL
3.3.7	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL

3.3.8	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL

3.4 Contract Management					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
3.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
3.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL

3.5 School Fund					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
3.5.1	School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2	School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3	School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6	School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7	School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL

3.6 School Meals Management					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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	Yes if letting details relate to individual		Current financial year + 6 years	SECURE DISPOSAL

4.2 Maintenance					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
4.2.1	All records relating to the maintenance of the school carried out by contractors	Yes if contractor details relate to individual		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	Yes if employee details shown		Current year + 6 years	SECURE DISPOSAL

5. Pupil Management

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

5.1 Pupil's Educational Record					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
5.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	Limitation Act 1980 (Section 2)	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 disposed of under instructions of the examination board
	Internal			This information should be added to the pupil file	
5.1.3	Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4	Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and	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	SECURE DISPOSAL – these records MUST be shredded

			promote the welfare of children March 2015"	found on the Local Authority Social Services record	

5.2 Attendance					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
5.2.1	Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2	Correspondence relating to authorised absence	Yes	Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
5.3.1	Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Yes	Children and Family's Act 2014; Special Educational Needs and Disability Act 2001 (section 14)	Date of Birth of the pupil + 31 years	REVIEW NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum

					retention period and this should be documented.
5.3.2	Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3	Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold

6. Curriculum Management

6.1 Statistics and Management Information					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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
	Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL
6.1.3	SATS records	Yes		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.	SECURE DISPOSAL
6.1.4	Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5	Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.6	Self-Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.7	Internal Moderation	Yes		Academic year + 1 academic year	SECURE DISPOSAL
6.1.7	External Moderation	Yes		Until superseded	SECURE DISPOSAL

6.1 Implementation of Curriculum					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
6.2.1	Schemes of Work	No		Current year + 1 year	REVIEW 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 of homework set	No		Current year + 1 year	

6.2.6	Pupils' Work	Yes if identifiable		current year + 1 year if work not returned to pupil	SECURE DISPOSAL

7. Extra Curricular Activities

7.1 Educational Visits outside the Classroom					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
7.1.1	Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.2	Parental consent forms for school trips where there has been no major incident.	Yes		Conclusion of the trip	SECURE DISPOSAL 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
7.1.3	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	DOB of the pupil involved in the incident + 25 years	SECURE DISPOSAL 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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period

7.2.1	Walking Bus Registers	Yes	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	Date of register +3 years [If these records are retained electronically any back up copies should be destroyed at the same time]	SECURE DISPOSAL

7.3 Family Liaison Officers and Home School liaison Assistants					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
7.3.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL
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	SECURE DISPOSAL
7.3.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
7.3.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
7.3.5	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
7.3.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL

8. Central Government and Local Authority

This section covers records created in the course of interaction between the school and the local authority

8.1 Local Authority					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
8.1.1	Secondary Transfer Sheets	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					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period	Action at End of Retention Period
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

Appendix 3: CCTV Procedure

1. Introduction

1.1 Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the Data Protection legislation regardless of the number of cameras or how sophisticated the equipment is.

1.2 This CCTV policy explains how Aylesbury Grammar School will operate its CCTV equipment and comply with the current legislation.

2. Why we use CCTV

2.1 The school uses CCTV equipment to provide a safer, more secure environment for students and staff and to prevent bullying, vandalism and theft. Essentially, it is used for:

- The prevention, investigation and detection of crime.
- The apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings).
- Safeguarding public, student and staff safety.
- Monitoring the security of the site.

2.2 The school does not use the CCTV system for covert monitoring.

3. Location and Specification

3.1 Cameras are located in those areas where the school has identified a need and where other solutions are ineffective.

3.2 The school's CCTV system is used solely for purposes identified above and is not used to routinely monitor staff conduct.

3.3 Cameras will only be used, in exceptional circumstances, in areas where the subject has a heightened expectation of privacy e.g. changing rooms or toilets. In these areas, the school will use increased signage in order that those under surveillance are fully aware of its use.

3.4 In areas where CCTV is used the school will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

3.5 The signs will be clearly visible and readable.

3.6 The school's standard CCTV cameras record visual images only and do not record sound.

3.7 If two way audio feeds (e.g. call for help systems) are used, they will only be capable of activation by the person requiring help.

4. Administration

4.1 The school has responsibility for the control of images and deciding how the CCTV system is used.

4.2 All employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.

4.3 Access to recorded images are restricted to staff that need to have access in order to achieve the purpose of using the equipment.

4.4 Staff accessing the images will follow procedures with regard to access to and disclosure of the recorded images

4.5 If the recorded image reveals misconduct by a member of staff, this evidence may be used in a disciplinary case.

5. Image storage, viewing and retention

5.1 Recorded images will be stored securely within the school that ensures the integrity of the image and in a way that allows specific times and dates to be identified

5.2 Access to live images is restricted to authorised staff unless the monitor displays a scene which is in plain sight from the monitored location.

5.3 Recorded images will only be viewed in a restricted area by authorised staff.

5.4 The school reserves the right to use images captured on CCTV where there is an activity that the school cannot be expected to ignore such as criminal activity, potential misconduct or behaviour which puts others at risk.

5.5 Images retained for evidential purposes will be retained in a secure area accessible by the system administrator.

5.6 Where images are retained, the system administrator will ensure the reason for its retention, where stored, any use made of the images and when finally destroyed are recorded.

5.7 Images will normally only be kept for 30 days unless required for evidential purposes.

6. Disclosure

6.1 Disclosure of recorded images to third parties can only be authorised by the data controller (the school) in accordance with Data Protection legislation.

6.2 All requests for access or disclosure are recorded and if access or disclosure is denied, the reason will be documented.

7. Subject access requests

7.1 Under Data Protection legislation and Freedom of Information Act, individuals, whose images are recorded, have a right to view images of themselves and be provided with copy of those images.

7.2 The school will respond to the request within the statutory time limits.

7.3 If the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed as personal data and any disclosure will be in accordance with the Data Protection legislation.

7.4 Those requesting access must provide enough detail to allow the school to identify that they are the subject of the images and locate the images on the system.

7.5 Requests for access should be made to the school's Data Protection Officer.