Data Protection (including records management) and Freedom of Information Policy

Document Control:

This document has been approved for operation within:	Apex Collaborative Trust		
Status	Statutory		
Owner	Apex Collaborative Trust		
Date effective from	June 2026	**Date of next review**	June 2027
Review period	Annually	**Version**	2

Version	Changes identified
2	DPO updated to SPoc throughout the policy Age of consent for photographs and videos changed to 12

Contents

1. Aims

Schools within Apex Collaborative Trust aim 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 UK General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and guidance

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

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

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

This policy also complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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 • 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

Apex Collaborative Trust processes personal data relating to parents, pupils, staff, governors, visitors and others within their schools, and therefore is a data controller.

The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Board of Trustees

The Trustees have overall responsibility for ensuring that schools within Apex Collaborative Trust complies with all relevant data protection obligations and have delegated responsibility to the CEO.

5.2 Single Point of Contact/Data protection Officer

The Single Point of Contact (SPoC) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The Trust's SPoC is Ms W Hamilton and is contactable via GDPRenquiries@apex-trust.org.

They will provide termly reports of their activities directly to the governing body and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

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

The Trust DPO is Veritau. Veritau can be contacted below:

West Offices
Station Rise
York
North Yorkshire
YO1 6GA
schoolsDPO@veritau.co.uk
01904 554025

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the SPoC in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that schools within Apex Collaborative Trust must comply with.

The principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed
6. Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK 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.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule/records management policy.

8. Sharing personal data

We will not normally share personal data with anyone else, except for those reasons contained within the privacy notice and where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

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

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

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

If staff receive a subject access request, they must immediately forward it to the SPoC.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children **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 pupils at Schools within Apex Collaborative Trust may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children **below the age of 12** are generally **not** regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils at Schools within Apex Collaborative Trust may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Important Note about Educational Records: a subject access request is different than a request from a parent to see their son/daughter's educational records. All parents have the right to see their child's educational record within 15 school days.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

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

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Parental requests to see the educational record

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

11. CCTV

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

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

Any enquiries about the CCTV system should be directed in the first instance to Ms Hamilton (SPoC).

12. Photographs and videos

(This section has a specific policy and procedures that need to be read in conjunction)

As part of Apex Collaborative Trust activities, we may take photographs and record images of individuals within Apex Collaborative Trust schools.

We will obtain written consent from parents/carers, or pupils aged 12 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil 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 individual school or Trust websites 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. In line with best practice for schools in managing images and videos, Trust schools will ensure that any meta data locations not linked to the school site or a school visit site will be removed.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of within Apex Collaborative Trust and the DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords to access school computers, laptops and other devices will be at least 8 characters long containing letters and numbers and a special character. Staff and pupils will be required and reminded to change their passwords at termly intervals
- No portable devices and removable media will be used – data must be saved on the cloud platform.

- Staff, pupils or governors who store personal information on their personal devices will be expected to follow the same security procedures as for school-owned equipment.
- If personal data is taken off site, then it will be subject to the same security procedures as when it is at school. Any data breaches whilst off site will be put under the same investigation procedures as if the breach was on site and subject to the same consequences.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

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

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

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

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff training will be provided, including data protection training as part of their induction process.

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

18. Monitoring arrangements

The SPoC is responsible for monitoring and reviewing this policy.

This policy is in line with UK GDPR and the Data Protection Bill that received royal assent on 25 May 2018 (Data Protection Act 2018) –This policy will be reviewed annually and shared with the full governing body.

19. Links with other policies

This data protection policy is linked to our:

- Acceptable use of ICT policy

- Child protection and safeguarding policy
- CCTV policy
- Retention policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the SPoC. The SPoC will investigate the report and determine whether a breach has occurred. To decide, the SPoC 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 SPoC will alert the headteacher and the chair of governors
- The SPoC 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 SPoC will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The SPoC 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 SPoC will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the SPoC must notify the ICO.
- The SPoC will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the SPoC will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the SPoC 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 SPoC 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 SPoC expects to have further information. The SPoC will submit the remaining information as soon as possible
- The SPoC 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 SPoC 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 SPoC
    - 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 SPoC 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 SPoC will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school's computer system.

  The SPoC and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the SPoC as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the SPoC will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the SPoC will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The SPoC will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The SPoC will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

Appendix 2: Freedom of Information (FOI) and Environmental Information Regulation (EIR) Requests

Freedom of Information (FOI)

The Freedom of Information Act 2000 (FOIA) is part of the Government's commitment to greater openness and transparency in the public sector. It enables members of the public to scrutinise the decisions of public authorities more closely and ensure that services are delivered properly and efficiently. Schools have two main responsibilities under the Freedom of Information Act:

- To publish certain information about its activities in a publication scheme, and
- To process and respond to individual requests for information, with a duty to provide advice and assistance.

Under FOI, anyone can request access to general recorded information we hold. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings. A Code of Practice under section 45 of the Act sets out recommendations for the handling of requests for information. To comply with this Code requests must:

- Be in writing,
- Provide the name or company name and contact address or email address,
- Describe the information they are requesting,
- Ideally, state the preferred format they would like the information to be provided.

Any request that cannot be answered promptly as part of normal day to day business or where we are asked to handle it under Freedom of Information, will be treated as a FOI request.

Information can be withheld if one or more of the 24 exemptions within the FOIA apply. This could mean that certain information is not released in response to a request or is not published. Requests for information can be refused for reasons including:

- The information is not held.
- It would cost too much or take too much staff time to comply with the request.
- The request is considered vexatious.
- The request repeats a previous request from the same person.

Requests for information under FOI and EIR

Any requests received should be forwarded to GDPRenquries@apex-trust.org who will log and acknowledge the request.

The SPoC is responsible for:

- Deciding whether the requested information is held,
- Locating, retrieving or extracting the information,

- Considering whether any exemption or exception might apply, and the balance of the public interest test,
- Preparing the material for disclosure and drafting the response,
- Seeking any necessary approval for the response and sending the response to the requester.

FOI requests must be made in writing. We will only consider requests which provide a valid name and address, and we will not consider requests which ask us to click on electronic links.

Appendix 3: Surveillance and CCTV Policy

This policy concerns our use of surveillance technology and related processing of personal data. It is written in accordance with data protection and human rights legislation and relevant codes of practice.

Surveillance is the close observation or monitoring of individuals or spaces, for the purpose of influencing behaviour or protecting people. We only use surveillance in the context of CCTV and e-monitoring software. We do not operate covert surveillance technologies and therefore this policy does not cover the use of such technology.

CCTV

We operate Closed Circuit Television (CCTV) systems to:

- Protect school buildings and property.
- Protect the safety and wellbeing of pupils, our workforce and visitors.
- Deter and discourage anti-social behaviour such as bullying, theft and vandalism.
- Monitor compliance with school rules and policies.
- Support the police in the prevention, detection, investigation and prosecution of any crimes.

E-monitoring

We operate e-safety monitoring software systems to:

- Safeguard our pupils and staff.
- Promote wellbeing and early intervention.
- Ensure appropriate use of school assets and resources.
- Monitor compliance with school rules and policies.

Privacy Risk Assessment

Under the UK GDPR, we are required to consider and address privacy implications to data subjects when implementing new data processing systems. This is known as privacy by design. The usual method for assessing privacy risks to individuals is by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is mandatory for surveillance activities since they are deemed particularly intrusive. We will ensure that DPIAs have been completed for both CCTV and e-monitoring and that there are no unmitigated high risks to the rights and freedoms of data subjects. In addition, we will review and update the relevant DPIA if we substantively change our systems.

We will ensure we have completed the Privacy by Design checklist for call recording.

Contract Management

We are required to have contracts with any data processors we use, containing certain data processing clauses prescribed by law. We will ensure that we have implemented an appropriate contract with the providers of our CCTV and e-monitoring systems to allow for them storing,

monitoring or accessing the data on our behalf. We will only agree to these contracts where they have been assessed for compliance and determined to meet our requirements.

Transparency
The use of CCTV systems must be visibly signed. Signage will include the purpose of the system, the name of the organisation operating the system and details of who to contact about the system. The signage will be clear and kept unobstructed, so that anyone entering the area will be aware that they are being recorded.

The use of e-monitoring systems must also be clearly signed. Users will be made aware of the e-monitoring by a notice on the log in screen of computers and it is also clearly detailed in the ICT Acceptable Use Policy.

Access Controls
Surveillance system data will only be accessed to comply with the specified purpose. For example, footage of CCTV systems intended to prevent and detect crime will only be examined where there is evidence to suggest criminal activity has taken place. Logs of e-monitoring systems intended to safeguard children will only be examined where there is reasonable cause to believe a child is at risk. Each system will have proportionate access controls and a nominated responsible person who will be accountable for the security of the system and authorise other specified staff members to access data held on the systems routinely or on an ad-hoc basis.

Disclosures
A request by an individual for surveillance data held about them will be treated as a subject access request (SAR). For more information on data subjects' right of access to their information, please refer to our Data Protection Policy.

If we receive a request for surveillance data from an official agency, such as the police, then we will confirm the purpose of the request and their lawful basis for accessing the data. We may also require formal documentation in support of the request. We will liaise with our Data Protection Officer (DPO) if we have any concerns about such requests.

Record of Processing and Retention
We have a duty under Article 30 of the UK GDPR to ensure that all our data processing activities are recorded for accountability purposes. We maintain an Information Asset Register to fulfil this requirement. We will ensure that the use of surveillance systems is detailed on this register.

Surveillance records will only be held as long as necessary to fulfil the specific purpose and deleted in line with our Records Management Policy.

Reviews
CCTV systems must be reviewed annually to ensure that systems still comply with data protection legislation and national standards. The IAO should use the checklist included in Appendix A of this policy to complete this review.

The school should review the e-monitoring systems regularly by undertaking a review of the DPIA and updating the DPIA to reflect any changes in how the system is used or the type of data that is collected.

The school should review the call recording systems regularly by undertaking a review of the Privacy by Design checklist and updating it to reflect any changes in how the system is used.

Complaints
Complaints by individuals about the use of surveillance systems or data will be treated as a data protection concern. For more information on data protection complaints, refer to our Data Protection Policy.

Appendix 4: Management of the School Records

1. **Governance**

1.1	Governance of the Academy Trust				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
1.1.1	Appointment of Trustees, Governors and Directors	Yes		Life of appointment + 6 years	SECURE DISPOSAL
1.1.2	Accessibility Plan	There may be if the plan refers to specific pupils	Limitation Act 1980 (section 2)	Life of plan + 6 years	SECURE DISPOSAL
2.1	**Board of Directors, Members Meetings and Governing Body**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
	Board of Directors				
1.2.1	Board Meeting Minutes	Could be if the minutes refer to living individuals	Companies Act 2006 (section 248)	Minutes must be kept for at least 10 years from the date of the meeting	OFFER TO ARCHIVES
1.2.2	Board Decisions	Could be if the decisions refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
	Committees				
1.2.3	Minutes relating to any committees set up by the Board of Directors	Could be if the minutes refer to living individuals		Date of the meeting + a minimum of 10 years	OFFER TO ARCHIVES
	General Members' Meeting				
1.2.4	Records relating to the management of General Members' Meetings	Could be if the minutes refer to living individuals	Companies Act 2006 (section 248)	Minutes must be kept for at least 10 years from the date of the meeting	OFFER TO ARCHIVES
1.2.5	Records relating to the management of the Annual General Meeting	Could be if the minutes refer to living individuals	Companies Act 2006 (section 248)	Minutes must be kept for at least 10 years from the date of the meeting	OFFER TO ARCHIVES

	Governors				
1.2.6	Agenda for Governing Body meetings	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
1.2.7	Minutes of, and papers considered at, meetings of the Governing Body and its committees	May be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal set (signed)			Life of Academy	
	Inspection copies			Date of meeting + 3 years	SECURE DISPOSAL
1.2.8	Reports presented to the Governing Body	May be data protection issues if the meeting is dealing 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 for the life of the Academy	SECURE DISPOSAL or retain with the signed set of minutes
1.2.9	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
	Statutory Registers[1]				
1.2.10	Register of Directors		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL

[1] Academies are required by law to keep specific records, collectively known as statutory registers or the statutory books. The registers record information relating to the Academy's operations and structure, such as the current directors. Records should be kept up-to-date to reflect any changes that take place.

1.2.11	Register of Directors' interests [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.12	Register of Directors' residential addresses		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.13	Register of gifts, hospitality and entertainments		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.14	Register of members		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.15	Register of secretaries		Companies Act 2006	Life of the Academy + 6 years	SECURE DISPOSAL
1.2.16	Register of Trustees' interests			Life of the Academy + 6 years	SECURE DISPOSAL
1.2.17	Declaration of Interests Statements [Governors] [this is not a statutory register]			Life of the Academy + 6 years	SECURE DISPOSAL
1.3	**Funding and Finance**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
	Payroll and Pensions				
1.3.1	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
1.3.2	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	Regulation 15 Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI1995/3103)	From the end of the year in which the accounts were signed for a minimum of 6 years	SECURE DISPOSAL
1.3.3	Management of the Teachers' Pension Scheme	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.4	Records relating to pension registrations	Yes		Date of last payment on the pension + 6 years	SECURE DISPOSAL
1.3.5	Payroll records	Yes		Date of payroll run + 6 years	SECURE DISPOSAL
1.3.6	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
1.3.7	School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
1.3.8	School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
1.3.9	School Fund – Bank statements	No		Current year + 6 years	SECURE DISPOSAL
	School Meals[2]				
1.3.10	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
1.3.11	School meals registers	Yes		Current year + 3 years	SECURE DISPOSAL

[2] Unless it would be unreasonable to do so, school lunches should be provided when they are requested by, or on behalf of, any pupil. A school lunch must be provided free of charge to any pupil entitled to free school lunches. From September 2014, free school lunches must be provided to all KS1 pupils.

2. Human Resources

2.1	Recruitment[3]				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.1.1	All records leading up to the appointment of a new Head Teacher	Yes		Date of appointment + 6 years	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 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	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 added to the Staff Personal File	SECURE DISPOSAL
2.1.5	Pre-employment vetting information – Evidence proving the right to work in the United Kingdom[4]	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, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment plus not less than 2 years	SECURE DISPOSAL
2.1.6	Records relating to the employment of overseas teachers	Yes		Where possible, these documents should be added to the Staff Personal File, but if they are kept separately, then the Home Office requires that the documents are kept for termination of employment	SECURE DISPOSAL

[3] Academies do not necessarily have to employ people with qualified teacher status; only the SEN and designated LAC teacher must be qualified.
[4] Employers are required to take a "clear copy" of the documents which they are shown as part of this process.

				plus not less than 2 years	
2.1.7	Records relating to the TUPE process	Yes		Date last member of staff transfers or leaves the organisation + 6 years	SECURE DISPOSAL
2.2	**Operational Staff Management**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.2.1	Staff Personal File, including employment contract and staff training records	Yes	Limitation Act 1980 (section 2)	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**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.3.1	Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded[5]	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"	Until the person's normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	SECURE DISPOSAL These records must be shredded
	Disciplinary proceedings	Yes			
2.3.2	Oral warning			Date of warning + 6 months[6]	SECURE DISPOSAL[7]
2.3.3	Written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL
2.3.4	Written warning – level 2			Date of warning + 12 months	SECURE DISPOSAL
2.3.5	Final warning			Date of warning + 18 months	SECURE DISPOSAL

[5] This review took place when the Independent Inquiry on Child Sexual Abuse was beginning. In light of this it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention.
[6] Where the warning relates to child protection issues, see above. If the disciplinary proceedings relate to a child protection matter, please contact your Safeguarding Children Officer for further advice.
[7] If warnings are placed in personal files, then they must be weeded from the file.

2.3.6	Case not found			If the incident is child protection related then see above; otherwise, dispose of at the conclusion of the case	SECURE DISPOSAL
2.4	**Health and Safety**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
2.4.1	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
2.4.2	Accident reporting	Yes	Social Security (Claims and Payments) Regulations 1979 (regulation 25). Social Security Administration Act 1992 (section 8). Limitation Act 1980	The official Accident Book must be retained for 3 years after the last entry in the book. The book may be in paper or electronic format. The incident reporting form may be retained as below.	
	• Adults			Date of incident + 6 years	SECURE DISPOSAL
	• Children			Date of birth of the child + 25 years	SECURE DISPOSAL
2.4.3	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL

3. Management of the Academy

3.1	**Admissions**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.1.1	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
3.1.2	Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory Guidance for admission authorities,	Resolution of case + 1 year	SECURE DISPOSAL

			governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014		
3.1.3	Register of admissions	Yes	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities October 2014 (page 6)	Every entry in the admission register must be preserved for a period of 3 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
3.1.4	Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL
3.1.5	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
3.1.6	Supplementary information form, including additional information such as religion and medical conditions	Yes			
	• Successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
	• Unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL
3.2	**Head Teacher and Senior Management Team**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.2.1	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		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

		or members of staff			
3.2.2	Minutes of Senior Management Team meetings and 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
3.2.3	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
3.2.4	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
3.2.5	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
3.2.6	Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
3.3	**Operational Administration**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
3.3.1	Management of complaints	Yes		Date of complaint resolved + 3 years	SECURE DISPOSAL

3.3.2	Visitors' books and signing in sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL

4. 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.

Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule

4.1	Pupil's Educational Record				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
4.1.1	Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 (SI 2005 No. 1437)		
	• Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when they leave the primary school. This will include: • To another primary school • To a secondary school • To a pupil referral unit If the pupil dies whilst at primary school, the file should be returned to the LA 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 LA 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 LA, as it is more likely that the pupil will request the record from the LA.
	• Secondary		Limitation Act 1980 (section 2)	Date of birth of the pupil + 25 years	SECURE DISPOSAL
4.1.2	Records relating to the management of exclusions	Yes		Date of birth of the pupil involved + 25 years	SECURE DISPOSAL
4.1.3	Management of examination registrations	Yes		The examination board will usually mandate how long these records need to be retained	
4.1.4	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	
4.1.5	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
4.1.6	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 promote the welfare of children March 2015"	Date of birth 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 LA Social Services record	SECURE DISPOSAL – these records MUST be shredded
4.2 Attendance					

	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [Operational]	Action at end of administrative life of the record
4.2.1	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 3 years after the date on which the entry was made	SECURE DISPOSAL
4.2.2	Correspondence relating to authorised absence		Education Act 1996 (section 7)	Current academic year + 2 years	SECURE DISPOSAL
4.3	**Special Educational Needs**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
4.3.1	Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (section 2)	Date of birth of the pupil + 25 years	REVIEW Note: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time in order 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 – this should be documented
4.3.2	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
4.3.3	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
4.3.4	Accessibility strategy	Yes	Special Educational Needs and Disability Act 2001	Date of birth of the pupil + 25 years [This would normally be	SECURE DISPOSAL, unless the document is

			(section 14)	retained on the pupil file]	subject to a legal hold

5. Curriculum Management

5.1	Statistics and Management Information				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
5.1.1	Examination results (schools copy)	Yes		Current year + 6 years	SECURE DISPOSAL
5.1.2	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
5.1.3	Published Admission Number (PAN) reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.1.4	Value added and contextual data	Yes		Current year + 6 years	SECURE DISPOSAL
5.1.5	Self-evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6. Extracurricular Activities

6.1	Educational Visits outside the Classroom				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
6.1.1	Parental consent forms for school trips where there has	Yes		Conclusion of the trip	Although the consent forms could be retained for date of birth + 25 years, the requirement for them being needed is low and most schools

	been no major incident[8]				do not have the storage capacity to retain every single consent form issued by the school for this period of time
6.1.2	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (section 2)	Date of birth 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	
6.1.3	Records relating to residential trips	Yes		Date of birth of youngest pupil involved + 25 years	SECURE DISPOSAL
6.2	**Walking Bus**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
6.2.1	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. Central Government and Local Authority (LA)

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

7.1	**Local Authority**				
	Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at end of administrative life of the record**
7.1.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
7.1.2	Attendance returns	Yes		Current year +1 year	SECURE DISPOSAL

[8] One-off or blanket consent: The Department for Education (DfE) has prepared a one-off consent form to be signed by the parent on enrolment of their child in a school. this form is intended to cover all types of visits and activities where parental consent is required. The form is available on the DfE website for establishments to adopt and adapt, as appropriate, at www.gov.uk/government/publications/consent-for-school-trips-and-other-off-site-activities. A similar form could be used or other establishments, such as Early Years Foundation Stage (EYFS) providers and youth groups, or at the start of programme for young people.

8. Financial Management of the School

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

8.1 Risk Management and Insurance					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.1.1	Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
8.2 Asset Management					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.2.1	Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
8.2.2	Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
8.3 Accounts and Statements including Budget Management					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.3.1	Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
8.3.2	Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
8.3.3	Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL

8.3.4	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
8.3.5	Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
8.3.6	Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
8.3.7	Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
8.4 Contract Management					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
8.4.1	All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
8.4.2	All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 years	SECURE DISPOSAL
8.4.3	Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
8.6 School Meals Management					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**

8.6.1	Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
8.6.2	School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
8.6.3	School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

9. Property Management

This section covers the management of buildings and property.

9.1 Property Management					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**
9.1.1	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	
9.1.2	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.	
9.1.3	Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
9.1.4	Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
9.2 Maintenance					
Basic file description		**Data Protection Issues**	**Statutory Provisions**	**Retention Period [Operational]**	**Action at the end of the administrative life of the record**

9.2.1	All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
9.2.2	All records relating to the maintenance of the school carried out by school employees including maintenance logbooks	No		Current year + 6 years	SECURE DISPOSAL