General Data Protection Policy (GDPR)

Document Control	
Title	Data Protection Policy
Date	June 2026
Supersedes	Version 3
Amendments	Section 11 CCTV Appendix 4
Related Policies/Guidance	Freedom of information publication scheme https://www.cherrytreetrust.org.uk/serve_file/10726409 Online Safety Policy https://www.newallgreen.manchester.sch.uk/serve_file/26896792

Approved by:	Trust Board	Date: 21.07.26
Last reviewed on:	June 2026	
Next review due by:	June 2027	

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2. Legislation and guidance

This policy meets the requirements of the:

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

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

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

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

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.

TERM	DEFINITION
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

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

The school is registered with the ICO and has paid its data protection fee, as legally required.

5. Roles and Responsibilities

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.

5.1 Governing Board

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

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Dianne Harris and is contactable via email, admin@newallgreen.manchester.sch.uk .

5.3 Senior Leadership Team Member

A Senior Leadership Team Member acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

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

The principles say that personal data must be:

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

This policy sets out how the 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 basis' (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 pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

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

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

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals about a child or themselves as a parent, we will provide them with the relevant information required by data protection law which is on the parent / school agreement form. The consent is recorded on Sims.

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.

Annually we inform the staff of the information that we hold and the need for holding the information. The staff sign on to their SSS account to tick to verify that they agree to us holding their information.

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.

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

In addition, 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, see Appendix 2.**

8. Sharing Personal Data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. **We have general consent through the Parent / School Agreement form but we will always seek verbal consent at the time a referral needs to be made unless information is being shared with partner agencies as part of safeguarding processes.**

These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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

- For some sharing (e.g., safeguarding), consent is not always needed if there's a legal basis. GOV.UK
- For statutory data submissions (like the school census), the school is required to share certain data by law, so consent is not needed for that

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

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.
When a child moves to another school we will send the CTF files and CPOMs information as this is required for the next educational establishment to comply with their legal duties.

9. Subject Access Requests (SARs)

9.1 General Rights

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

Subject access requests can be submitted in any form, but we may be able to respond more efficiently if requests are made in writing and include:

- The individual's name
- Correspondence address
- Contact number and/or email address
- Details of the information requested

If staff receive a subject access request in any form, they must immediately forward it to the Data Protection Officer (DPO).

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, not to 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 for the parent/carer to act on their behalf.

Children below the age of 12 are generally not regarded as mature enough to understand their rights and the implications of a subject access request. Therefore, most SARs from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a fixed rule, and a pupil's understanding will always be assessed on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to SARs, we will:

- Verify the requester's identity, and may ask for two forms of identification.
- Contact the requester by telephone or email to confirm that the request was made.
- Respond without undue delay and within one month of receipt of the request (or receipt of identification, where relevant).
- Extend the response time by up to two additional months where the request is complex or numerous. We will inform the individual within one month if this applies and explain the reason for the extension.
- Provide the information free of charge, unless the request is manifestly unfounded, excessive, or repetitive, in which case we may charge a reasonable fee to cover administrative costs or refuse to act on the request.

If we refuse a request, we will explain why, and inform the individual of their right to complain to the ICO or seek to enforce their rights through the courts.

We may not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that a child is being, or has been, abused, or is at risk of abuse, where disclosure would not be in the child's best interests.
- Includes another person's personal data that cannot be reasonably anonymised, and where consent has not been obtained, and it would be unreasonable to disclose without it.
- Is part of sensitive or exempt records (e.g. crime, immigration, legal proceedings, management forecasts, confidential references, or examination scripts).

9.4 Managing SARs: Key Areas to Consider

1. Reasonable and Proportionate Searches

The school will conduct *reasonable and proportionate* searches for personal data. This requirement will become statutory once the relevant provisions of the Data Protection and Digital Information (No. 2) Act (DUAA) take effect.

Searches should be targeted and efficient. If keyword searches reveal excessive or irrelevant results, search terms will be refined. While requesters may suggest search terms or locations, the school is not legally bound to follow these instructions, provided it meets the reasonable and proportionate search threshold.

2. Safeguarding Information

Requests involving safeguarding information—such as those linked to allegations, bullying, or welfare concerns—will be carefully managed. There is no blanket safeguarding exemption; however, exemptions may apply where disclosure would not be in the child's best interests or could compromise safeguarding measures.

Decisions will prioritise the child's welfare, considering:

- Whether the child's views should be sought, particularly for older pupils.
- The impact of disclosure on other individuals (e.g., other pupils or staff).
- The applicability of exemptions to support the child's best interests.

3. Personal Data, Not Documents

A SAR grants access to *personal data*, not necessarily to the documents containing it. Where appropriate, the school may extract relevant personal data and present it in a structured format (e.g., a table or schedule) rather than disclosing full documents. This approach helps minimise redactions and prevent unnecessary disclosure of third-party data.

4. Extending the Response Timeframe

The school may extend the response timeframe by up to two additional months where the request is complex. Complexity may arise from:

- A high volume of data or multiple data sources.
- The need to consult third parties or assess exemptions.
- The overlap of a request with school holiday periods.

  The school will inform the requester within one month if an extension is required, explaining the reason and expected completion date.

5. Managing Complaints

Under the DUAA, schools are required to have a formal process for handling data protection complaints, including those related to SARs.

If an individual is dissatisfied with the school's handling of their SAR, they may raise a complaint under the

school's internal Data Protection Complaint Procedure before escalating to the ICO. This ensures clarity for requesters and provides the school with a defined escalation pathway, reducing prolonged correspondence.

9.5 Other Data Protection Rights of Individuals

In addition to the right to make a subject access request, individuals have the right to:

- Withdraw consent to processing at any time.
- Request rectification, erasure, or restriction of processing of their personal data (in certain circumstances).
- Object to processing justified on the basis of public interest, official authority, or legitimate interests.
- Prevent use of personal data for direct marketing.
- Challenge decisions based solely on automated decision-making or profiling.
- Be notified of a data breach (in certain circumstances).
- Request the transfer of their personal data to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

All such requests must be submitted to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Academies, including free schools, and independent schools, such as ours: there is no automatic parental right of access to the educational record in your setting, but you can request this in writing and we may choose to provide this.

11. CCTV (Closed Circuit Television)

11.1 Purpose

The school uses CCTV systems to:

- Safeguard pupils, staff, visitors and contractors.
- Protect school property and assets.
- Assist with the prevention and detection of crime, anti-social behaviour and breaches of school policies.
- Support investigations into incidents affecting the safety, security or operation of the school.

The use of CCTV is carried out in accordance with the UK GDPR, Data Protection Act 2018 and the Information Commissioner's Office (ICO) guidance on video surveillance.

11.2 Ownership and Management

The CCTV system and all images, recordings and associated data remain the property of the school.

The Headteacher is responsible for the overall operation of the CCTV system.

The Data Protection Officer (DPO) is responsible for ensuring that CCTV footage is processed and disclosed in accordance with data protection legislation and this policy.

11.3 CCTV Signage

The school will clearly identify areas where CCTV is in operation through appropriate signage.

Individuals entering the site will be informed that CCTV is being used for security and safeguarding purposes.

11.4 Access to CCTV Footage

Access to live or recorded CCTV footage is restricted to authorised staff only.

Authorised staff may include:

- Headteacher
- Deputy Headteacher
- Data Protection Officer
- Site Manager
- Other staff specifically authorised by the Headteacher

Staff must only access CCTV footage where there is a legitimate business, safeguarding, health and safety, disciplinary, security or operational reason to do so.

All access to CCTV footage should be proportionate and limited to what is necessary.

The presence of a senior member of staff or the Data Protection Officer must not be assumed to constitute authorisation. Explicit authorisation must be obtained before CCTV footage is exported, copied or disclosed.

11.5 Requests to View CCTV Footage

CCTV footage may only be viewed where there is a legitimate safeguarding, behaviour, health and safety, security, operational or investigative reason.

Routine requests to view CCTV footage must be authorised by a member of the Senior Leadership Team.

Routine behaviour investigations may be authorised by any member of SLT. Staff must not independently access CCTV footage without authorisation, however a standing authorisation may be given to designated staff (e.g. Site Manager and Office Staff) to retrieve footage at the request of SLT.

All internal viewing of CCTV footage must be recorded in the CCTV Viewing Log (Appendix 3A).

Examples may include:

- Behaviour incidents
- Safeguarding concerns
- Accident investigations
- Site security incidents
- Property damage
- Staff welfare concerns

Viewing CCTV footage does not permit staff to download, copy, photograph, record or share footage.

11.6 Exporting CCTV Footage

The exporting, downloading or copying of CCTV footage is restricted to authorised staff only.

Authorisation must be obtained from the Headteacher, Deputy Headteacher or Data Protection Officer before footage is exported from the CCTV system.

Footage must only be exported where there is a legitimate purpose, including:

- Safeguarding investigations
- Formal disciplinary investigations
- Complaints investigations
- Police requests
- Insurance claims
- Legal proceedings
- Serious health and safety incidents

All exports of CCTV footage must be recorded in the CCTV Export and Disclosure Log (Appendix 3B).

Footage must be stored securely on school-controlled systems and must not be stored on personal devices.

11.7 Sharing CCTV Footage

CCTV footage contains personal data and must only be disclosed where there is a lawful basis to do so.

External disclosure must be authorised by the Headteacher, Deputy Headteacher or Data Protection Officer.

Before disclosure takes place, consideration must be given to:

- The lawful basis for disclosure
- The necessity and proportionality of the disclosure
- The rights and privacy of any individuals captured in the footage
- Whether redaction is required

All disclosures must be recorded in the CCTV Export and Disclosure Log (Appendix 3B).

The log must include:

- The recipient
- The purpose of the disclosure
- The authorising officer
- The method of transfer
- Any deletion or retention requirements

Where appropriate, recipients may be required to confirm deletion of footage once it is no longer required.

Under no circumstances may CCTV footage be disclosed through personal email accounts, personal mobile devices, text messages, WhatsApp or social media platforms.

11.8 Prohibited Activities

Under no circumstances may staff:

- Record CCTV footage using personal mobile phones, tablets or cameras.
- Photograph CCTV screens using personal devices.
- Store CCTV footage on personal devices.
- Transfer CCTV footage using personal email accounts.
- Share CCTV footage through WhatsApp, text message, social media or other personal communication platforms.
- Share CCTV footage without appropriate authorisation.

Failure to comply with these requirements may result in disciplinary action.

11.9 Police and External Agency Requests

Requests from the Police or other external agencies should be referred to the Headteacher or DPO.

Where footage is disclosed, the school will maintain a record of:

- The requesting organisation
- The lawful basis for disclosure
- The footage disclosed
- The date of disclosure

Where appropriate, written requests should be obtained and retained.

11.10 Subject Access Requests

Individuals may request access to CCTV footage containing their personal data through a Subject Access Request (SAR).

All requests must be referred immediately to the DPO.

The school will consider the rights of all individuals captured in the footage before any disclosure takes place.

11.11 Retention of CCTV Footage

CCTV footage will be retained only for as long as necessary to fulfil its purpose.
Routine CCTV recordings will normally be retained in accordance with the school's CCTV system settings unless required for an ongoing investigation, complaint, disciplinary matter, safeguarding concern or legal process.
Where footage is retained for evidential purposes, it will be securely stored and deleted once no longer required.

11.12 Data Breaches

Any loss, unauthorised access, unauthorised disclosure or inappropriate use of CCTV footage must be reported immediately to the DPO and dealt with in accordance with the school's Data Breach Procedure.
Staff must not attempt to conceal or resolve potential breaches themselves.

12. Photographs and Videos

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

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.
Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

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

13. Data Protection by Design and Default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14. Data Security and Storage of Records

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

In particular:

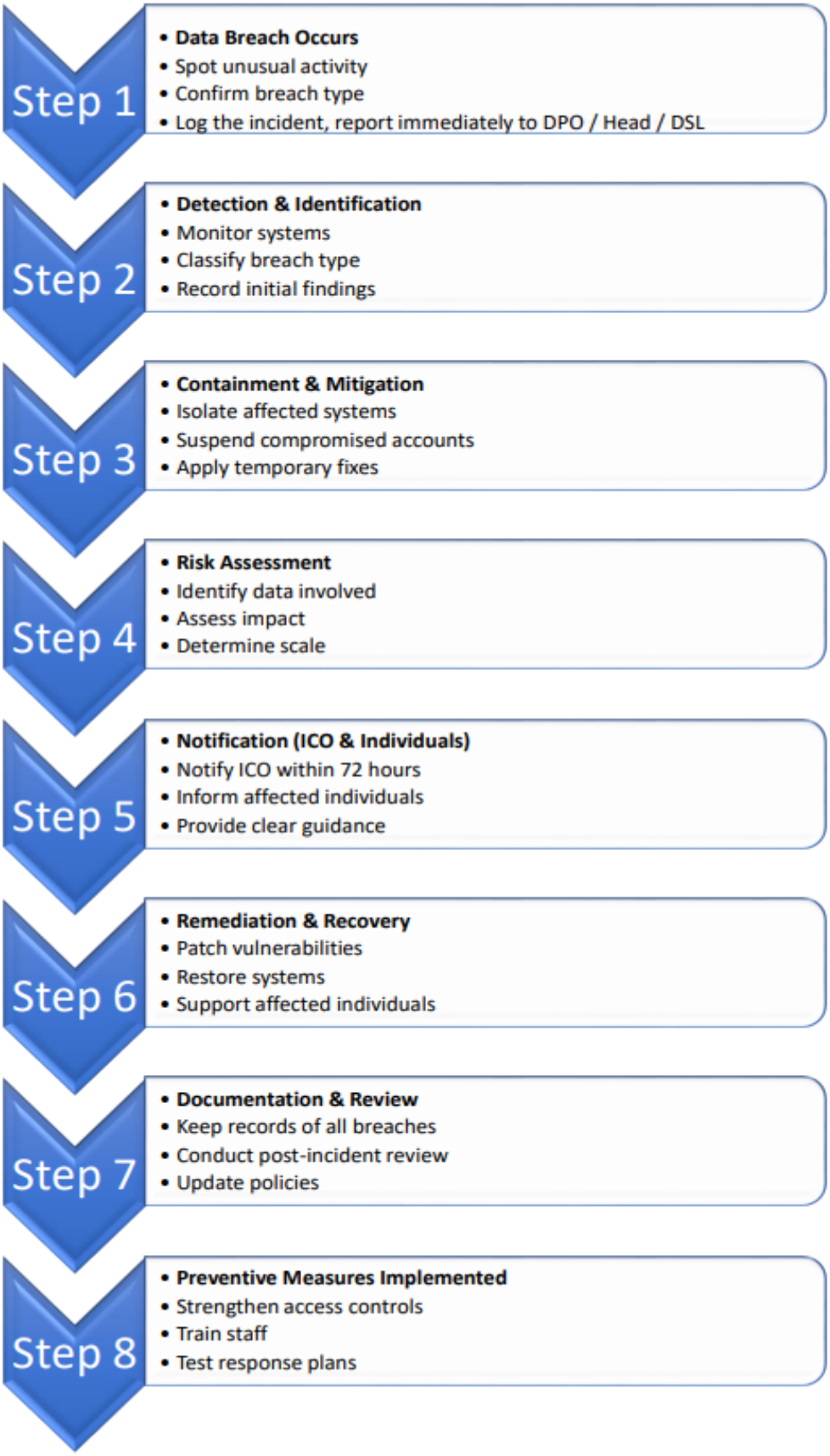
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, it must be used on a password protected on-line app or laptop with log in systems.
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded 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, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Social Media and IT 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

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 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 pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. Training

All staff and governors are provided with data protection training as part of their induction process.
Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

18. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- **Online Safety Policy**

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email to admin@newallgreen.manchester.sch.uk .
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert a member of the Senior Leadership Team Member and the Chair of Trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).

    - Remove incorrect email recipients' access.
    - Lock user accounts if login credentials were compromised.
    - Recover USB sticks or physical files.
    - Shut down affected systems if required.
    - **Staff must never try to hide a breach** — they are required to escalate it.

- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences

- What personal data is involved? (e.g., names? medical info? SEND? safeguarding? staff disciplinary data?)
- Whose data was affected? (pupils, staff, parents, vulnerable individuals, etc.)
- How sensitive is it?
- How many people are affected?
- Has the data been accessed by someone unauthorised?
- Is the data recoverable?
- What harm could occur? (risk to safety, distress, reputational harm, identity fraud, safeguarding concerns)

› The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

- Safeguarding records emailed to the wrong parent
- SEND or medical files disclosed publicly
- Loss of an unencrypted laptop containing pupil data
- Staff payroll information leaked
- Breaches not usually reportable:
- An email containing only names sent to the wrong internal staff member
- Minor admin errors where no harm is likely
- If unsure: the default is to contact the DPO for assessment.
- You must document all breaches, even those not reported.

› The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the DPO's school's computer system.

› Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned
  - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

For example, you should contact individuals when:

- Safeguarding or child protection data is exposed
- Medical or SEND details have been compromised
- Passport/birth certificate/ID scans are lost
- Addresses or contact details of vulnerable pupils are revealed

Notifications should be:

- Clear and plain English
- Explain what happened, what data is affected, and what the school is doing
- Provide contact details for the school/DPO
- Offer advice on how individuals can protect themselves (if relevant)

Do not downplay the breach — transparency is essential.

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

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

- The DPO and a member of the Senior Leadership Team Member will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Mitigate the Impact

Depending on the breach, this may include:

- Resetting passwords
- Recalling emails / restricting shared links
- Retrieving hard copies
- Asking recipients to delete data and confirm deletion
- Strengthening technical security (encryption, multi-factor authentication)
- Providing support to affected individuals

- The DPO and a Senior Leadership Team Member will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that you might want to consider could include:

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

Appendix 2 Retention Information

Taken from https://www.securestorageservices.co.uk/article/19/white-paper-retention-guidelines-for-schools#:~:text=Retain%20in%20school%20for%206%20years%20from%20report%20date.

Secure Storage Services outline the Retention Guidelines for Schools (RGS) as prescribed by the Records Management Society of Great Britain. The RGS outlines recommended retention periods for a diverse class of records created by schools in the course of their operations.

Some of the below retention periods are governed by statute. We specifically state the relevant statutory provision where applicable. When the law is silent, retention periods outlined below are recommended as 'best practice'.

Following the guidelines set out in the RGS below will also ensure you are compliant with the Data Protection Act 1998 and the Freedom of Information Act 2000.

If you plan to retain or destroy documents for shorter or longer periods than stated below, you must retain documented reasons for doing so.

1. Records relating to child protection

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
1.1	Child protection files	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	Date of birth + 25 years	Secure disposal
1.2	Allegation of child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance). Education Act 2002 Guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	Secure disposal

2. Records relating to governors

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
2.1	Minutes -				
2.1a	Principal set (signed)	No		Permanent	Must be available in school for 6 years from the meeting. Can then be archived/stored elsewhere.
2.1b	Inspection copies	No		Date of meeting + 3 years	Secure disposal
2.2	Agendas	No		Date of meeting	Secure disposal
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from report date. Can consider archiving/storing anything important.
2.4	Annual parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from meeting date. Can consider archiving/storing anything important.
2.5	Instruments of Government	No		Permanent	Retain in school whilst school open. Can then be archived/stored elsewhere.
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required. Can then be archived/stored elsewhere.
2.7	Action plans	No		Date of action plan + 3 years	Secure disposal
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy operational (this includes if the expired policy is part of a past decision making process).
2.9	Complaints files	Yes		Date of resolution of complaint + 6 years	Review for further retention in the case of contentious disputes. Secure disposal.
2.10	Annual reports required by Dept of Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI2002 No1171	Date of report + 10 years	Secure disposal
2.11	Proposals for schools to become or be established as Specialist Status schools	No		Current year + 3 years	Secure disposal

3. Records relating to school management

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
3.1	Log books	Yes		Date of last entry in book + 6 years	Secure disposal
3.2	Minutes of the senior management team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in school for 5 years from meeting date. Can consider archiving/storing anything important.
3.3	Reports made by the head teacher or management team	Yes		Date of report + 3 years	Retain in school for 3 years from report date. Can consider archiving/storing anything important.
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes		Closure of file + 6 years	Secure disposal
3.5	Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No/Yes		Date of correspondence + 3 years	Secure disposal
3.6	Professional development plans	Yes		Closure + 6 years	Secure disposal
3.7	School development plans	No		Closure + 6 years	Review for further retention. Secure disposal.
3.8	Admissions - if the admission is successful	Yes		Admission + 1 year	Secure disposal
3.9	Admissions - if the appeal is unsuccessful	Yes		Resolution of case + 1 year	Secure disposal
3.10	Admissions - secondary schools - casual	Yes		Current year + 1 year	Secure disposal
3.11	Proof of address supplied by parents as part of the admissions process	Yes		As the corresponding admission record	Secure disposal
3.12	Supplementary information form including additional information such as religion, medical conditions supplied as part of the admissions process	Yes		As the corresponding admission record	Secure disposal

4. Records relating to pupils

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
4.1	Admission registers	Yes		Entry + 7 years	Retain in school for 7 years from entry. Can consider archiving these records if have the facility.
4.2	Attendance registers	Yes		Date of register + 3 years	Secure disposal
4.3	Pupil files retained in schools	Yes			
4.3a	Primary	Yes		Retain for time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.3b	Secondary	Yes	Limitation Act 1980	Date of birth + 25 years	Transfer to another secondary school if required. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit. Secure disposal
4.4	Pupil files	Yes			
4.4a	Primary	Yes		Retain for time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.4b	Secondary	Yes	Limitation Act 1980	Date of birth + 25 years	Transfer to another secondary school if required. In the case of exclusion it may be appropriate to transfer the record to the Pupil Referral Unit. Secure disposal
4.5	Special Educational Needs files, reviews and individual education plans	Yes		Date of birth + 25 years	Secure disposal
4.6	Correspondence relating to authorised absence and issues	Yes		Date of absence + 2 years	Secure disposal
4.7	Examination results				
4.7a	Public	No		Year of examination + 6 years	Secure disposal

4.7b	Internal examination results	Yes		Current year + 5 years	Secure disposal
4.8	Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and retain with pupil file if necessary. Secure disposal
4.9	Statement maintained under the Education Act 1996 Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	Date of birth + 30 years	Secure disposal unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	Date of birth + 30 years	Secure disposal unless legal action is pending
4.11	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	Secure disposal unless legal action is pending
4.12	Accessibility strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	Secure disposal unless legal action is pending
4.13	Parental permission slips for school trips, where there has been no major incident	Yes		Conclusion of the trip	Secure disposal unless legal action is pending
4.14	Parental permission slips for school trips, where there has been a major incident	Yes	Limitation Act 1980	Date of birth of pupil involved in the incident + 25 years	Secure disposal. Permission slips for all pupils on trip need to be retained for period to show that the rules had been followed for all pupils.
4.15	Records created by schools to obtain approval to run an educational visit outside the classroom, primary schools	No	3 part supplement of the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 14 years	Secure disposal
4.16	Records created by schools to obtain approval to run an educational visit outside the classroom, secondary schools	No	3 part supplement of the Health & Safety of Pupils on Educational Visits (HASPEV) (1998)	Date of visit + 10 years	Secure disposal
4.17	Walking bus registers	Yes		Date of register + 3 years	This takes into account that if an incident requiring an accident report, the register will be submitted with the accident report and kept for the retention time for accident reporting. Secure disposal

5. Records relating to child Curriculum

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
5.1	School development plan	No		Current year + 6 years	Secure disposal
5.2	Curriculum returns	No		Current year + 3 years	Secure disposal
5.3	Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.5	Class record books	Yes/No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.6	Mark books	Yes/No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.8	Pupils' work	Yes		Current year + 1 year	It may be appropriate to review these records at end of each year and allocate a new retention period. Secure disposal.
5.9	Examination results	Yes		Current year + 6 years	Secure disposal
5.10	SATs records, examination papers and results	Yes		Current year + 6 years	Secure disposal
5.11	PAN reports	Yes		Current year + 6 years	Secure disposal
5.12	Value added and contextual data	Yes		Current year + 6 years	Secure disposal
5.13	Self evaluation forms	Yes		Current year + 6 years	Secure disposal

6. Records relating to personnel records

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	Secure disposal
6.2	Staff personnel files	Yes		Termination + 25 years	Secure disposal
6.3	Interview notes and recruitment records	Yes		Date of interview notes + 6 months if unsuccessful. If successful place in personnel file.	Secure disposal
6.4	Pre-employment vetting information (including CRB checks)	Yes	CRB guidelines	Date of check + 6 months	Secure disposal
6.5	Disciplinary proceedings	Yes	Where the warning relates to child protection issues see 1.2		
6.5a	Oral warning	Yes		Date of warning + 6 months	Secure disposal
6.5b	Written warning - level one	Yes		Date of warning + 6 months	Secure disposal
6.5c	Written warning - level one	Yes		Date of warning + 12 months	Secure disposal
6.5d	Final warning	Yes		Date of warning + 18 months	Secure disposal
6.5e	Case not found	Yes		If child protection see 1.2, otherwise destroy immediately	Secure disposal
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years	In case of serious accidents a further retention period will need to be applied. Secure disposal
6.7	Annual appraisal and assessment records	Yes		Current year + 5 years	Secure disposal
6.8	Salary cards	Yes		Last date of employment + 85 years	Secure disposal
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI 1999/567)	Current year + 3 years	Secure disposal

6.10	Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	Secure disposal
6.11	Proofs of identity collected as part of the process for checking "portable" enhanced CRB disclosure	Yes		Where possible these should be checked and a note/copy of what was checked placed on personnel file. If felt necessary to keep any documentation this should also be placed in personnel file.	Secure disposal of notes/copies and return of originals.

7. Records relating to health and safety

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
7.1	Accessibility plans	Yes	Disability Discrimination Act	Current year + 6 years	Secure disposal
7.2	Accident reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		Secure disposal
7.2a	Adults	Yes		Date of incident + 7 years	Secure disposal
7.2b	Children	Yes		Date of birth of child + 7 years	Secure disposal
7.3	COSHH			Current year + 10 years	Where appropriate an additional retention period may be allocated. Secure disposal
7.4	Incident reports	Yes		Current year + 20 years	Secure disposal
7.5	Policy statements			Date of expiry + 1 year	Secure disposal
7.6	Risk assessments			Current year + 3 years	Secure disposal
7.7	Process of monitoring areas where employees and persons are likely to have come in contact with asbestos			Last action + 40 years	Secure disposal
7.8	Process of monitoring areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	Secure disposal
7.9	Fire precautions log book			Current year + 6 years	Secure disposal

8. Administrative records

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
8.1	Employer's liability certificate			Closure of school + 40 years	Secure disposal
8.2	Inventories of equipment and furniture			Current year + 6 years	Secure disposal
8.3	General file series			Current year + 5 years	Review to see if further retention period required. Secure disposal
8.4	School brochure or prospectus			Current year + 3 years	Disposal
8.5	Circulars (staff, parents, pupils)			Current year + 1 year	Review to see if further retention period required. Secure disposal
8.6	Newsletters, ephemera			Current year + 1 year	Review to see if further retention period required. Secure disposal
8.7	Visitors book			Current year + 2 year	Review to see if further retention period required. Secure disposal
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see if further retention period required. Secure disposal

9. Records relating to Finance

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
9.1	Annual accounts		Financial Regulations	Current year + 6 years	Secure disposal
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Secure disposal
9.3	Contracts				
9.3a	Under seal			Contract completion date + 12 years	Secure disposal
9.3b	Under signature			Contract completion date + 6 years	Secure disposal
9.3c	Monitoring records			Current year + 2 years	Secure disposal
9.4	Copy orders			Current year + 2 years	Secure disposal
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	Secure disposal
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	Secure disposal
9.7	Annual budget and background papers			Current year + 6 years	Secure disposal
9.8	Order books and requisitions			Current year + 6 years	Secure disposal
9.9	Delivery documentation			Current year + 6 years	Secure disposal
9.10	Debtors' records		Limitations Act	Current year + 6 years	Secure disposal
9.11	School fund - Cheque books			Current year + 3 years	Secure disposal
9.12	School fund - Paying in books			Current year + 6 years	Secure disposal
9.13	School fund - Ledger			Current year + 6 years	Secure disposal
9.14	School fund - Invoices			Current year + 6 years	Secure disposal
9.15	School fund - Receipts			Current year + 6 years	Secure disposal

9.16	School fund - Bank statements			Current year + 6 years	Secure disposal
9.17	School fund - School journey books			Current year + 6 years	Secure disposal
9.18	Student grant applications	Yes		Current year + 3 years	Secure disposal
9.19	Free school meals registers	Yes		Current year + 6 years	Secure disposal
9.20	Petty cash books			Current year + 6 years	Secure disposal

10. Records relating to property

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
10.1	Title deeds			Permanent	These should follow the property
10.2	Plans			Permanent	Retain in school whilst operational. Can then be archived/stored elsewhere.
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	Secure disposal
10.4	Leases			Expiry of lease + 6 years	Secure disposal
10.5	Lettings			Current year + 3 years	Secure disposal
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	Secure disposal
10.7	Maintenance log books			Last entry + 10 years	Secure disposal
10.8	Contractors' reports			Current year + 6 years	Secure disposal

11. Records relating to local authorities

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
11.1	Secondary transfer sheets (primary)	Yes		Current year + 2 years	Secure disposal
11.2	Attendance returns	Yes		Current year + 1 year	Secure disposal
11.3	Circulars from LEA	Yes		Whilst required operationally	Review to see if further retention period required. Disposal

12. Records relating to the Department of Education

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
12.1	HMI reports			These do not need to be kept any longer	Secure disposal
12.2	OFSTED reports and papers			Replace former report with new inspection report	Review to see if further retention period required. Secure disposal
12.3	Returns			Current year + 6 years	Secure disposal
12.4	Circulars from Department of Education			Whilst required operationally	Review to see if further retention period required. Disposal

13. Records relating to working agreements

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
13.1	Service level agreements			Until superseded	Secure disposal
13.2	Work experience agreement	Yes		Date of birth of child + 18 years	Secure disposal

14. Records relating to school meals

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
14.1	Dinner register			Current year + 3 years	Secure disposal
14.2	School meals summary sheets			Current year + 3 years	Secure disposal

15. Records relating to Family Liaison Officers and Home School Liaison Assistants

	Basic File Description	Data Protection Issue	Statutory Provisions	Retention Period	Action at End of Administrative Life of Record
15.1	Day books	Yes		Current year + 2 years	Review to see if further retention period required. Secure disposal
15.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school	Secure disposal
15.3	Referral forms	Yes		While the referral is current	Secure disposal
15.4	Contact data sheets	Yes		Current year then review	If contact is no longer active secure disposal
15.5	Contact database entries	Yes		Current year then review	If contact is no longer active secure delete
15.6	Group registers	Yes		Current year + 2 years	Secure disposal

Appendix 3 Data Breach Incident Report Form

1. Basic Information

Date breach discovered:

Time breach discovered:

Name of person reporting the breach:

Role / Job title:

Contact details:

2. Description of the Incident

What happened?

How was the breach discovered?

Date and time the breach occurred (if known):

Location of breach:

3. Type of Breach

Loss of data

Unauthorised access

Unauthorised disclosure

Accidental destruction

Alteration of data

Cyber incident (e.g., phishing, malware, ransomware)

Other:

4. Categories of Personal Data Affected

Basic personal data (name, address, email)

Financial data

Special category data (health, SEND, ethnicity, safeguarding)

Staff HR data

Pupil data

Parent/carer data

Images / CCTV

Login credentials / passwords

Other:

5. Individuals Affected

Approx. number of individuals affected:

Types of individuals affected: Pupils / Staff / Parents / External / Other:

6. Immediate Containment Actions

What steps were taken to contain the breach?

Is the data recoverable? Yes / Partially / No

7. Initial Risk Assessment

Potential harm resulting from breach:

Sensitivity of data involved: Low / Medium / High

Likelihood of harm: Unlikely / Possible / Likely

Overall risk level: Low / Medium / High

8. ICO Reporting Decision

Does this breach meet the threshold for ICO reporting? Yes / No

If yes, date/time reported:

ICO reference number:

9. Notification to Individuals

Do affected individuals need to be informed? Yes / No

If yes, how and when they were informed:

Summary of message given:

10. Mitigation and Follow-up Actions

Steps taken to reduce future risk:

External agencies involved:

11. Lessons Learned

What went wrong?

What needs to change?

Responsible person for improvements:

Target date for completion:

12. Sign-off

Completed by (name):

Role:

Signature:

Date:

Reviewed by DPO:

Signature:

Date:

Appendix 4 CCTV Viewing Log

This log must be completed whenever CCTV footage is viewed for internal school purposes.

Date	Time	Requested By	Authorised By	Reason for Viewing	Location Viewed	Outcome/Action Taken

Examples of reasons:

- Behaviour incident
- Safeguarding concern
- Accident investigation
- Site security
- Property damage
- Staff concern

Appendix 4 - CCTV Export and Disclosure Log

Important: CCTV footage must never be photographed, filmed, downloaded to, stored on, or shared from a personal device. All exports and disclosures must be authorised and recorded using this log.

CCTV Access, Export and Disclosure Record

This log must be completed whenever CCTV footage is:

- Viewed for an investigation or incident.
- Downloaded or exported from the CCTV system.
- Shared internally beyond the authorised reviewing staff.
- Shared externally with any third party.

A separate form should be completed for each incident.

Section 1 – Incident Details

Date of Incident:

Time of Incident:

Location of Incident:

Brief Description of Incident:

Section 2 – Request Details

Name of Person Requesting CCTV Review:

Role:

Date Request Made:

Reason for Request:

☐ Safeguarding Concern

☐ Behaviour Incident

☐ Health & Safety Incident

☐ Security Incident

☐ Complaint Investigation

☐ Staff Investigation

☐ Police Request

☐ Insurance Claim

☐ Other

Details:

Section 3 – Authorisation to View Footage

Authorising Senior Leader:

Role:

Date Authorised:

Lawful Purpose for Viewing:

Authorisation Granted:

☐ Yes

☐ No

Signature:

Date:

Section 4 – CCTV Review

Date Footage Viewed:

Time Footage Viewed:

Names of Staff Viewing Footage:

1. ---
2. ---
3. ---

Summary of Findings:

Outcome:

☐ No Further Action

☐ Internal Follow-Up

☐ Safeguarding Action

☐ Behaviour Sanction

☐ Further Investigation Required

☐ Footage to be Exported

☐ Other

Details:

Section 5 – Export of Footage

Was Footage Exported?

☐ Yes

☐ No

If Yes:

Date Exported:

Exported By:

Storage Location:

☐ School Network

☐ Encrypted School Device

☐ Police Evidence Request

☐ Other Approved Location

File Reference Number (if applicable):

Reason for Export:

Section 6 – Disclosure of Footage

Was Footage Shared Outside School?

☐ Yes

☐ No

If Yes:

Name of Recipient:

Organisation:

Reason for Disclosure:

Lawful Basis for Disclosure:

Authorised By:

Role:

Date Shared:

Method of Transfer:

☐ Secure School Email

☐ Encrypted File Transfer

☐ Police Evidence Portal

☐ Secure Cloud Link

☐ Other Approved Method

Details:

Confirmation of Receipt Obtained?

☐ Yes

☐ No

Confirmation of Deletion Required?

☐ Yes

☐ No

Date Confirmation Received:

Section 7 – Data Protection Compliance Check

I confirm that:

☐ Access was authorised.

☐ Footage was viewed only for a legitimate purpose.

☐ No personal devices were used.

☐ Footage was stored securely.

☐ Any disclosure was authorised and recorded.

☐ Data protection requirements have been followed.

Completed By:

Role:

Signature:

Date:

Section 8 – DPO Review (where applicable)

Reviewed By:

Role:

Date:

Comments:

Action Required:

☐ None

☐ Training

☐ Policy Review

☐ Data Breach Investigation

☐ Other

Details: