St Catherine's
CE PRIMARY SCHOOL

Data Protection (GDPR) Policy



Policy version number:	2
Date policy written:	August 2025
Author:	Kris Edwards & Julie Cook
Next Review:	August 2027
Approved by & date:	SLT

1. Purpose

St Catherine's CE Primary School Data Protection Policy is intended to ensure that personal information is dealt with securely and in accordance with the Data Protection Act 2018, UK General Data Protection Regulation (GDPR). It will apply to all data held by the school regardless of the way it is used, recorded and stored and whether it is held by the school in paper files or electronic form.

2. Introduction

The General Data Protection Regulation (GDPR) forms part of the Data Protection Act 2018. This regulation identifies certain principles that any organisation who stores or processes 'Personally Identifiable Information' must be able to demonstrate compliance with. The GDPR applies to all electronic and manual data files containing personally identifiable information (PII) or sensitive data.

St Catherine's CE Primary School collect and use certain types of personal information about pupils, parents, staff, volunteers, governors, job applicants and other individuals who come into contact with the school in order to provide education, employment and other associated functions. Our school is required by law to collect and use certain types of information to comply with statutory obligations related to education, safeguarding and employment, and this policy is intended to ensure that personal information is dealt with securely and in accordance with the GDPR.

This policy has been put into place to ensure all Staff and Governors who process PII in the school understand the scope of the regulation, how it affects them, and the working practices that must be employed on a day-to-day basis in order to safeguard the personal information of individuals, which we have and use within the school. St Catherine's CE Primary School will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this policy and their duties under the GDPR and should ensure they refer to this policy when carrying out their duties. St Catherine's CE Primary School will take all reasonable steps and apply robust procedures to ensure that all PII is held securely and is not accessible to unauthorised persons.

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO).

This policy will be updated when amendments to the data protection legislation are made or to reflect best practice where necessary. The policy will be reviewed every 2 years.

3. Definitions and Common Terminology

- ***Data Controller*** – a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The school is a data controller for the purposes of GDPR.

- ***Data Processor*** – a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller. This applies to third party organisations who process data on behalf of the school.
- ***Data Subject*** – an identified or identifiable living individual whose personal data is held or is processed. In relation to school this includes, staff, parents, carers, pupils, volunteers, governors, visitors etc.
- ***Personally Identifiable Information*** – any information relating to an identified or identifiable, living individual.
- ***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.
- ***Data Protection Officer*** – a person who is tasked with helping to protect personally identifiable information and helping an organisation to meet the GDPR compliance requirements, does not hold ultimate accountability for compliance.
- ***Subject Access Request*** – a right that a person has to obtain a copy of information held about them by the organisation.
- ***Data Breach*** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.
- ***ICO*** – Information Commissioners Office (Supervising Authority in the UK)

4. Principles and How St Catherine's CE Primary School Complies

In accordance with the obligations placed upon the school as a Data Controller, personal data will be processed in accordance with the Principles of GDPR. The following section outlines how St Catherine's CE Primary School processes personal data in line with the GDPR guiding principles as follows:

4.1 Legality, Transparency and Fairness: *Personal data will only be processed by the school, where it is able to demonstrate that it has a 'Lawful Basis' for the processing activity. Personal data will be processed fairly, and the school are open and honest about the uses of personal data.*

A data mapping document is a 'live' document that records all data processed by the school. A 'Lawful Basis' is recorded against each data set to evidence and record a legal reason for collecting, processing, sharing, storing, and destroying data.

The data mapping document will be held by the school business manager. All staff will be required to assist periodic reviews of the data mapping document to ensure all data sets currently in use within the school have been considered, captured, and a lawful basis for processing has been identified on each occasion.

A Privacy Notice details the school's use of personal data, including what PII is held by the school, how it will be stored, the organisations that data will be shared with, the lawful basis for processing and how long the data will be held for prior to destruction. Our data mapping

document informs the content of our privacy notices. It also contains information regarding how a data subject (pupil, parent, member of staff etc) can access their data, which is stored and processed by the school.

In accordance with the principal of transparency, the school has developed and will maintain privacy notices for different categories of data subject. These outline the categories of data captured, the purpose of processing and if the information is shared with third party organisations.

Privacy notices for the following categories of data subjects and details of where this information is available, is as follows:

- Pupils, Parents and Carers: available via our school website
- Staff: available via Shared drive
- Visitors and Contractors: available via school website
- School Governors: available via staff share
- Job Applicants: available via school website

A Data Subjects Rights

Under the GDPR, data subjects have the following rights with regards to their personal information, as follows:

1. Right to be informed about the collection and the use of their personal data
2. Right of access personal data and supplementary information
3. Right to have inaccurate personal data rectified, or completed if it is incomplete.
4. Right to erasure (to be forgotten) in certain circumstances.
5. Right to restrict processing in certain circumstances
6. Right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across difference services.
7. Right to object to processing in certain circumstances.
8. Rights in relation to automated decision making and profiling.
9. Right to withdraw consent at any time (where relevant)
10. Right to complain to the Information Commissioner

Individuals can submit a request to exercise the above rights to the Data Protection Lead in school. This may be done verbally or in written form. If staff receive such a request, they will immediately forward it to the Data Protection Lead, who will liaise with the Data Protection Officer as necessary. See section 8 for details of how a data subject can exercise their right to access their personal data.

4.2 Purpose Limitation: *Personal data should be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.*

A data mapping document will identify the purposes for which processing will take place, the description of the categories of individuals and personal data, the categories of recipients of the data (e.g., Third party organisations who the school shares the data with). Retention schedules for the personal data will also be noted.

Appropriate technical and organisational measures must be in place to safeguard personal data and ensure PII is only used for the purpose for which it was collected.

4.3 Minimisation: *The personal data must be 'Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.'*

Data collection forms and processes will be regularly reviewed to ensure information is appropriate and not excessive. Data required by teaching staff will be provided only for the purpose it is required to ensure data used is minimal.

If a member of staff wishes to introduce the use of new technology that captures personally identifiable information, they will first speak with the data protection lead in school. The Data Protection Lead will ensure appropriate measures, including completion of a data Protection Impact assessment prior to approval of a project and identify the appropriate lawful basis. The data mapping document will be updated accordingly.

Wherever there is any uncertainty about the level of information being requested from Data Subjects, a referral will be made to the Data Protection Lead/Officer for further guidance.

4.4 Accuracy: *All reasonable steps will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*

Data will be proactively and regularly checked to ensure it is as accurate as possible through a variety of measures:

- Issuing data capture forms on an annual basis to parents/carers to verify the accuracy of personal information held on the SIMS system, including emergency contact details; correspondence address; medical details of the pupils etc.
- During termly parents' evenings
- Termly newsletters to remind parents to update their data if required.
- Checking the accuracy of data during contact with parents including first day calling conversation via SENCO etc.
- Checking attainment data in systems on a regular basis, through the use of pupil progress meetings;
- Checking accuracy of staff details via Schoalr pak

- **4.5 Storage Limitation:** *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*

Retention periods for various data held in the school are recorded within the data mapping document. The school refer to the Information Record Management Toolkit to establish appropriate retention periods and data is archived and destroyed as set out in these guidelines (See appendix 1 - Data Retention Schedule).

Personal data that is no longer required either due to it being out of date, inaccurate or in line with the school retention policy, will be disposed of securely.

The school will put paper-based records into the confidential bin and delete electronic files. School may also use a third-party organisation to safely dispose of records on the school's behalf. If so, a third-party assurance certificate will be obtained to provide school with sufficient guarantees that the company complies with data protection law.

4.6 Integrity and Confidentiality: *Personal data will be processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

(a) Clear desk and clear screen:

- PCs must not be accessible to others. All electrical devices including laptops, iPads, must not be left unlocked when workstations/classrooms are left unattended.
- Computer screens will be positioned to ensure only authorised personnel are able to view sensitive or confidential information. This is of particular importance within areas accessed by members of the public, such as the reception area or main school office. Privacy screens will be used where positioning of screens is not possible.
- Any paper-based documents containing personally identifiable information will be secured in a lockable cabinet or cupboard when classrooms / offices are left unattended and always at the end of the day. Data will not be displayed on notice boards. Where there are any concerns over the availability of secure (lockable) storage, or clarification required over the type of information that needs to be secured, staff will speak with the Data Protection Lead in the first instance, who will liaise with the Data Protection Officer if required.

(b) Passwords and protection of hardware:

- Passwords for accessing systems will be complex enough to make it extremely difficult for third parties to break them: passwords will be at least 10 characters long, have a mixture of upper case and lower-case letters, at least one number and one character. Where applicable a two-step authenticator app will be used to ensure an extra layer of security.
- Passwords will be changed regularly, and never shared with any other member of staff / shared amongst other users or written down.
- Mobile devices (including phones, tablets and laptops) will be protected to the same high standard. School staff will:
- Activate the built-in security PIN and set this to the most secure level (if the device allows, this will always be a secure password as detailed above or fingerprint recognition rather than a 4-digit pin;
- A copy of the IMEI numbers for the phone and the SIMS are stored securely to allow deactivation in the event of loss.
- All school staff are personally responsible for any information accessed or disclosed on the devices they access. Therefore, passwords will be kept safe and secure, and will not be shared with anyone else, as outlined above.

(c) Accessing and sharing information:

- Electronic data will only be accessed via school devices. Staff are permitted to access emails or personal data via their own devices, including mobile phones, laptops, iPads/tablets etc. providing a password is set up. Refer to the ICT Acceptable Use Policy.
- Staff will follow the secure process of accessing data via Google Drive and how to safely download, modify, save and send data securely.
- Personal data will not be downloaded onto a personal mobile device without a justified clear business case for doing so and prior management approval. Downloaded data will automatically save to the device and therefore, if approval has been granted the data must be deleted immediately when it is no longer required.

(d) Sharing of Personally Identifiable Information.

- **Inside the School:** Information of a confidential, sensitive or personal nature will only be shared with staff who require access to the information. Where data has been shared via email the data will be deleted by all staff once it has been used for the purpose it has been collected and is no longer required.
- **Outside the School:** Where more than one piece of personal, sensitive or confidential data is to be sent, one of several methods will be used. If in doubt staff will check with the Data Protection Lead.
- Secure transmission: Where possible, use recognised secure electronic exchange programmes.
- Never send personal data within a normal email. If email is the only method of transmission available, ensure the information is included in a password protected document. The password must be agreed with the email recipient in advance either face to face or via telephone. The password will not be shared in a follow-on email. The password will not be included in the email to which the password protected document is attached (if the first email is intercepted, then the second could also be).
- Checks will be carried out prior to data being shared with third parties as to the purpose and only appropriate data will be provided. Staff will check with the Data Protection Lead before any data is shared.
- Data will be checked for accuracy and to ensure it is current prior to sending.
- School emails will never be sent to individuals within an organisation using a public email address (e.g., Hotmail, Gmail etc.) regardless of what they contain, unless this has been clearly identified by the recipient as their business email address and prior approval given by school SLT.
- Emails sent to a number of recipients will be checked for accuracy prior to sending. Parent's emails addresses will be inserted into the blind copy (BCC) section of the email to protect individuals contact details being shared.
- When sending information (including letters) via post the following process will be followed:

- A second person will always check the address is correct prior to sending. Particular attention to house numbers is required as these are easily transposed. However, the responsibility for the accuracy is still with the sender not the checker.
- Window envelopes will be used if the address is pre-populated on the enclosed letter to avoid transcription errors. Where plain envelopes are used typed labels will be used to avoid issues in relation to legibility of handwritten.
- Envelopes will be securely sealed. Using additional methods such as sticky tape, glue or staples if deemed necessary.
- The contents of the letter will be double checked to ensure that no additional information has been included that is not relevant e.g., something mistakenly attached or personal data of another individual. Only relevant data will be sent.
- The document will be checked for validity and accuracy.
- If a request is received from an outside agency such as the Police, this will be referred in the first instance to the Data Protection Lead.

(e) Storage of Data on Portable/External Devices

- The loss of any device that can send, store or retrieve data will be reported to your Data Protection Lead and the Data Protection Officer immediately.
- All devices provided by school to include mobile phone, laptop, memory stick, tablet, external hard drive, computer etc, will be encrypted, and care must be taken to safeguard the equipment against loss or damage. The password used to encrypt information will not be written down and will never be stored or transported with the device. Staff are reminded to change their passwords at regular intervals if a forced change of password is not set.
- All devices provided by the school will only be used for the purposes for which they were supplied.
- Unencrypted memory sticks to store data are not permitted by the school. Memory sticks that do not require a password to access the data contained on it will not be used and are not permitted by the school.
- Any storage devices no longer required, which may contain information that is surplus to requirements or any device that needs secure disposal should be returned to IT staff within the school or the Data Protection Lead in person.
- Media such as CDs or DVDs, which contain data and are no longer required will be physically destroyed by the IT Department/Data Protection Lead.
- 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.

(f) Paper and Manual Filing Systems

- Paper based (or any non-electronic) information will be assigned an owner. A risk assessment will identify the appropriate level of protection for the information being stored. Paper and files in the School will be protected by one of the following measures:

- Locked filing cabinets with restricted access to keys by appropriate staff only. Keys will be stored away from cabinets.
- Locked safes
- Stored in a secure area protected by access controls.
- Depending on the content of the sensitive data contained within papers and files, the appropriate member of staff will be responsible for the storing and protecting of the data in line with the secure filing system process.

(g) Security of Equipment and Documents Off School Premises

- Information storage equipment, such as computers, laptops, tablets, mobile phones and external storage devices will only be taken off school site if authorisation from the Head Teacher has been obtained.
- Personally identifiable information, sensitive or confidential data contained within paper-based documentation will only be taken off school site if authorisation from the Head Teacher has been obtained.
- Staff will adhere to the following security guidelines when taking equipment and/or documents off school site:
- Equipment/documents will not be left unattended in public places.
- Equipment/documents will not be left unattended in a vehicle unless the property is concealed from view and all doors are locked, windows and the roof closed and fastened, all security devices on the vehicle are put in full and effective operation and all keys/removable ignition devices removed from the vehicle.
- Equipment/documents will not be left open to theft or damage whether in school, during transit or at home.
- Where possible, equipment/documents will be stored discreetly (e.g., laptops should be carried in less formal bags)
- Equipment/documents will be returned to the school as soon as is practically possible.
- Data encryption will be in place, and manufacturer's instructions for protecting school equipment will be observed at all times.

(h) Physical Security

- This section is related to building security and the level of care that will be taken when transporting computers or paper files outside of the building.

- Data held by the school will be protected against the possibility that it could be stolen, lost or otherwise divulged by physical (or non-electronic) means. The following organisational security measures are in place to protect all sensitive, personally identifiable and confidential information:
- The school premises are protected by door locks and access codes. The codes remain secure and form part of the school's physical security procedures and as such help to keep personal, sensitive and confidential data safe.
- Doors and windows are locked when areas are left unattended and external doors (including loading bay/fire doors) are locked when not in use.

- All visitors sign in and receive a Visitor's Authentication Badge. This is issued by the staff in Reception and applies to all Visitors using Inventry system.
- All Visitors/Attendees will be supervised at all times and are required to wear visible authorised identification, and to record their date/time of entry/departure and person(s) being visited.
- Where personally identifiable, sensitive or confidential data is requested, staff will ensure it is a legitimate request and data is not breached. If in doubt, checks with the Data Protection Lead or the Data Protection Officer will be carried out.

(i) CCTV

- The school operates a CCTV system to monitor activities within and around school, to identify instances of criminal activity and to ensure the safety and wellbeing of the School community. The school do not need to ask the permission of individuals on the school site to record images on CCTV.
- The school will only operate overt surveillance and will display signs in the areas of the school where this is in operation. Covert surveillance (i.e., which is intentionally not shared with the individuals being recorded) is not condoned by the school.
- Any enquiries or complaints about the schools CCTV system should be directed towards the data protection lead in school (see point 8) in the first instance, who will investigate as required, and respond in accordance with the schools CCTV policy.
- For more details, please refer to the schools CCTV Policy

4.7 Accountability: *the Controller will be able to demonstrate compliance with the previous principles.* The school will do this by employing measures including:

(a) Data Protection Officer and Data Protection Lead

- A Data Protection Officer (DPO) is appointed to the school who has suitable knowledge and experience to fulfil this role and has a direct line of report through to the Head Teacher and Governing body for data protection related matters.
- On a day-to-day basis, the first point of contact within the school is the Data Protection lead. The Data Protection lead will liaise with the Data Protection Officer for advice and guidance as required.
- The DPO will undertake periodic monitoring activities to help ensure compliance with the regulation. They will be informed of any suspected data breach, and will help to investigate circumstances surrounding breaches, and ascertain whether they are required to be reported to the ICO.
- The DPO will be informed of any Subject Access Requests that are submitted to the school and will assist in making the response to the Data Subject.
- For our school, the Data Protection Officer is provided to us by SIPS Education and are contactable via gdpr@sipseducation.co.uk or 0121 296 3000.
- The schools Governing Body will be kept informed of the ongoing compliance via reports to the FGB which will include an overview of any data breaches that have

occurred along with actions taken, and any Subject Access Requests received and responded to.

(b) Staff and Governor Training

- Annual training for staff and governors is provided. In addition to this, regular reminders to staff on the content and expectations of this policy and the procedures to follow to safeguard personal data is carried out.

(c) Third Party Organisations

- Where the school needs to share personal data with third party organisations (Data Processors), it will ensure that adequate checks have been undertaken on the robustness of the processors data protection systems to safeguard the information shared and will maintain a written record of this.

(d) Data Protection Impact Assessment

- Data Protection will be considered as part of all project planning when the school are reviewing systems for data collection and data processing. Where required, the school will undertake Data Protection Impact Assessments to ensure appropriate measures are put in place to safeguard the data, prevent breaches and ensure compliance with the requirements of the Regulation.

5. Photographs and Videos

The school may take photographs and videos of individuals as part of school activities. Such images may be used for:

- Notice boards around school, school newsletters, brochures etc
- External agencies such as the school photographer, newspapers/media campaigns
- School website or social media

In order to do this, we will obtain written consent from parents / carers before we take photographs or videos of your child. We will do this at the start of every academic year we seek your consent, we will clearly explain how the photographs and/or videos are to be used.

You have the right to withdraw consent at any time, upon which we will delete any images already taken and we will not distribute those images further.

As part of our 'public task,' we may take a photograph of your child without requesting consent from you. This would be in circumstances where identification of a child with an existing medical condition/allergy is required to meet the needs of your child and to keep them safe.

Where photographs and/or videos are taken by parents / carers at school events for their own personal use, the requirements of data protection legislation do not apply. However, we do ask that should your photos / videos capture images of other pupils in addition to their own child, that these are not shared in any public way (including on social media sites) for safeguarding reasons unless all relevant parents / carers have given their consent for them to do so.

6. Data Security and Storage of Data

All devices used in school and provided to staff including laptops will be encrypted. Care will be taken to safeguard the equipment against loss or damage. Passwords used on all devices to encrypt information, will not be shared or written down.

All devices provided by the school will only be used for the purposes for which they were supplied.

Memory sticks that do not require a password to access the data contained on it will not be used and are not permitted by the school.

Any storage devices no longer required, which may contain information that is surplus to requirements, or any device will be disposed of securely.

Paper based documents and files containing personal data, which is stored in School will be protected by one of the following measures:

- Locked filing cabinets with restricted access to keys by appropriate staff only.
- Keys will be stored away from cabinets.
- Locked safes
- Stored in a secure area protected by access controls.

Depending on the content of the sensitive data contained within papers-based documents and files, an appropriate member of staff will be responsible for the storing and protecting of the data in line with the secure filing system process.

7. Data Retention Schedule

The Data Retention Schedule (Appendix 1) which forms part of this policy, draws on recommended “best practice” retention periods from the IRMS Schools Toolkit and the Department for Education Data Protection Toolkit for Schools as well as relevant statutory provisions referenced within the schedule.

8. Subject Access Requests

Individuals (Data Subjects) 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 purpose 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 is not possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restrictions, 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
- The safeguards provided if the data is being transferred internationally.

It is important to bear in mind that a child's personal data is just that – their data – and does not belong to their parent / carer. As such, if a parent or carer wishes to make a subject access request for data relating to their child, the pupil will need to have given their consent depending on their age and level of understanding.

The age of 13 is used as a guide to determine when a child is generally likely to be mature enough to understand their rights, and accordingly any requests for their personal data from this age onwards would generally be expected to come from the child themselves.

For children below this age, it is less likely that they will fully understand the implications of a SAR, and so it would normally be acceptable for the request to come from the parent / carer.

Both above situations are used as a guide only, and each request (and requestor) will be assessed on an individual case by case basis.

Subject access requests can be submitted in any form to any member of staff within the school. However, the school may contact the requester for more details in order for the school to respond to requests appropriately. If staff receive a subject access request in any form, they will forward to the data protection lead within the school immediately. The data protection officer will also be advised to ensure appropriate support is provided to the school to fulfil the request.

Parents and staff can also contact the data protection lead within the school to make a subject access request via office@stcatherines.worcs.sch.uk

Information about how to make a Subject Access Request or for more details can be obtained from the Data Protection Lead within the school – Mrs K Edwards.

8.1 Responding to a Subject Access Request

When responding to requests, the school may:

- contact the individual via telephone to confirm the request has been made by them.
- ask the individual to provide further details so that the school can verify and confirm the data required.
- request 2 forms of identification of the individual. Proof of address will also be verified.
- If a third party is requesting data, written authority or a power of attorney will be verified.

Requests will be responded to within 1 calendar month from receipt of the request. However, if additional information is required for the school to fulfil the request the response period will be from receipt of all information obtained. This includes receipt of proof of identity and proof of address where relevant.

Based on the complexity of the request and in line with Article 12 (3) GDPR, the timeframe in which to respond to a Subject Access Request may be extended up to 3 calendar months if required. In such instances the school will liaise with the Data Protection Officer and liaise with the requester to advise of the response time or any delays at the earliest opportunity.

Data provided to the requester may contain details of other individuals and therefore such data will be redacted (blanked out) to protect those individuals' identity and personal data. Details contained within the documents will pertain to the appropriate individual only.

When responding to the request, the school may decide against disclosing information for a variety of reasons, including if it;

- would have an adverse effect on the rights and freedom of others.
- includes information that might cause serious harm to the physical or mental health of the pupil or another individual;
- includes information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests;
- includes information contained in adoption and parental order records;
- includes certain information which may be used in legal proceedings;
- would include personal data relating to another individual, where; the school cannot sufficiently anonymise the data to protect that individual's rights,' we do not have their consent to release that individuals' data, and it would be unreasonable to proceed without such consent.
- Safeguarding information recorded on safeguarding systems if release of the data could have the potential to cause serious harm to an individual or a live, legal process.

If a request is determined to be 'excessive or vexatious' the school has the right to refuse the request, or in some cases, charge a reasonable fee to cover the administrative costs of responding to the request.

If the school refuses a request, they will inform the individual of the reasons why and advise them of their right to complain to the ICO, if they wish to do so.

9. Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. The school has robust procedures in place to deal with any personal data breach and will notify the ICO where we are legally required to do so. Data subjects will be notified in instances where the rights and freedoms of such individuals has been compromised. The school will work with their Data Protection Officer to address a breach and school processes will be reviewed to mitigate risks if it is appropriate to do so.

9.1 Responding to Data Breaches

If any member of staff becomes aware of a data breach situation, they will ensure this is reported to the Data Protection Lead as soon as possible. The school will keep a record of all breaches and investigate them to an appropriate level, to ascertain what can be learnt from the circumstances surrounding each. Upon completion of an investigation procedures will be reviewed as required with the aim of preventing a similar breach occurring again.

Some breaches of a more serious nature will need to be reported to the ICO. The DPO will help the school to ascertain whether a breach is reportable and will advise on all such occasions if this is the case. The Data Protection Lead will liaise with the DPO to determine whether a breach is reportable to the ICO.

Where breaches are reportable, the school is legally required to submit the report to the ICO within 72 hours of the school becoming aware of the breach, and therefore staff members must advise the Data Protection Lead as soon as a breach is realised.

A near miss will also be reported to the DPL so that the school can learn from these and use them as a way of informing future revisions to our policies and/or procedures for data protection.

10. Complaints to the Information Commissioner

Should individuals be dissatisfied with the way the school has handled a request and want to make a complaint, they may write to the Information Commissioner, who is an independent regulator. Any complaint to the Information Commissioner is without prejudice to their right to seek redress through the courts.

The Information Commissioner can be contacted at:

Information Commissioners Office, Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF
Tel: 0303 123 1113

Website: https://ico.org.uk

11. Contact Details

If a data subject wishes to make a Subject Access Request (see point 8) or have general queries in relation to data protection within school, these should be directed to the Data Protection Lead within the school office@stcatherines.worcs.sch.uk

In the first instance concerns, questions or complaints, can be discussed with the Data Protection Officer at gdpr@sips.co.uk or telephone number 0121 296 3000. This would include situations where there are concerns about the way a Subject Access Request or a data breach has been addressed or the robustness of policy or procedures within school in relation to Data Protection.

If a data subject remains dissatisfied with the assistance that they have received or if they do not feel their subject access request has been dealt with appropriately or have concerns with regards to a possible breach, they can make a formal complaint to the Information Commissioners Office. This can be done via the website at www.ico.org.uk. Telephone: 0303 123 1113 or in writing to the Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire

Appendix 1

Data Retention Schedule					
1. Contracts					
Document	**Personal Information**	**Retention Period**	**Statutory Provisions**	**Disposal**	**Good Practice**
All records relating to the management of contracts under seal	No	Last payment on the contract + 12 years or end of contract + 12 years, whichever is the longer	Limitation Act 1980	SECURE DISPOSAL	irms Toolkit for Schools
All records relating to the management of contracts under signature	No	Last payment on the contract + 6 years or end of contract + 6 years whichever is the longer	Limitation Act 1980	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the management of contracts with external providers	No	End of contract + 6 years or date of last payment on contract + 6 years whichever is the longer		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the monitoring of contracts	No	End of the contract or until the final payment has been made whichever is the longer		SECURE DISPOSAL	irms Toolkit for Schools
All records relating to the maintenance of the school carried out by contractors	No	Current year + 6 years. This may vary on the type of maintenance. Records relating to rewiring, major alterations etc must be retained in the health and safety file whilst the building belongs to the school and must be passed onto any new owners if the building is leased or sold.		SECURE DISPOSAL	irms Toolkit for Schools
All records relating to the maintenance of the school carried out by school employees, including maintenance log books	No	Life of equipment + 6 years. Alterations to wiring and major modifications must be entered in to the health and safety file		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the management of software licences	No	Date licence expires + 6 years		SECURE DISPOSAL	irms Toolkit for Schools

2. Education Management

2.1 Management Information

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Published Admission Number (PAN) reports	Yes	Current year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Self Evaluation Forms - External moderation	Yes	Until superseded		SECURE DISPOSAL	irms Toolkit for Schools
Value added and contextual data	Yes	Current year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
2.2 Policies and Frameworks					
Complaints Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Data Protection Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Freedom of Information Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Information Security Breach Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Special Educational Needs Policy	No	Life of the policy or policy superseded + 3 years. If major changes are made to the policy then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Equality Information and Objectives (public sector equality duty). Statement for publication	No	Life of statement or date statement superseded + 3 years		SECURE DISPOSAL	irms Toolkit for Schools
Risk and Control Framework	No	Life of framework or framework superseded + 3 years. If major changes are made to the framework then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Rules and Bylaws	No	Life of rules or bylaws or rules or bylaws superseded + 3 years. If major changes are made to the rules or bylaws then an archive copy of previous policies should be retained		SECURE DISPOSAL	irms Toolkit for Schools
2.3 Strategy					
Strategic Review	No	Life of the review or until review superseded + 3 years. If major changes are made to the review then an archive copy of previous review should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Strategic Plan [also known as School Development Plans]	No	Life of plan or until plan superseded + 3 years.If major changes are made to the plan then an archive copy of previous plans should be retained		SECURE DISPOSAL	irms Toolkit for Schools
Accessibility Plan	No	Life of plan or plan superseded + 3 years the review. If major changes are made to the plan then an archive copy of previous policies should be retained Life of plan plus 6 years	Equality Act 2010 Limitation Act 1980	SECURE DISPOSAL SECURE DISPOSAL	irms Toolkit for Schools DfE Data Protection in Schools
2.4 Examinations					
SATs records Examination papers	Yes	The examination papers should be kept until any appeals/validation process is complete		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
SATs records Results	YES	The SATS results should be recorded on the pupils 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	irms Toolkit for Schools
2.5 Extra curriculum and miscellaneous activities					
Records created by schools in order to obtain approval to run an educational visit outside the classroom - Primary schools	No	Date of Visit + 15 years 10 years from the date of the visit. If there was an incident on the visit, retain the permission slips for all pupils and the incident report in the pupil record	Limitation Act 1980 Limitation Act 1980	SECURE DISPOSAL SECURE DISPOSAL	irms Toolkit for Schools DfE Data Protection in Schools
Parental consent forms for school trips where there has been no major incident	Yes	Conclusion of the trip. Although the consent forms could be retained for date of birth + 25 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form issued by the school for this period of time		SECURE DISPOSAL	irms Toolkit for Schools
Parental permission slips for school trips where there has been a major incident	Yes	Date of birth of the pupil involved in the incident + 25 years or 15 years after the incident whichever is the longer. 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	Limitation Act 1980	SECURE DISPOSAL	irms Toolkit for Schools
Records relating to residential trips	Yes	Date of birth of youngest pupil involved + 25 years or if there is a major incident then date of incident + 15 years whichever is the longer	Limitation Act 1980	SECURE DISPOSAL	irms Toolkit for Schools

3. Finance

3.1 Funding

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Funding Agreement with Secretary of State and supplemental funding agreements [Where there is multi-Academy governance.]	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Funding Agreement Termination of the funding agreement	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Funding Records Capital Grant	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Funding Records Earmarked Annual Grant (EAG)	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Funding Records General Annual Grant (GAG)	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Per pupil funding records	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Funding records	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Gift Aid and Tax Relief	Yes	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Exclusions agreement	No	Date of last payment of funding + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to loans	No	Date of last payment on loan + 6 years if the loan is under 10,000 or date of last payment on loan + 12 years if the loan is over 10,000		SECURE DISPOSAL	irms Toolkit for Schools
Management of Endowment Funds	No	Life of the fund + 6 years		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Investment policies	No	Life of the investment+ 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Pupil Premium Fund records	Yes	Date pupil leaves the provision + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Student Grant applications	Yes	Current year + 3 years		SECURE DISPOSAL	irms Toolkit for Schools
3.2 Operational					
Invoices, receipts, order books and requisitions, delivery notices	No	Current financial year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the collection and banking of monies	No	Current financial year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the identification and collection of debt	Yes	Payment or write off of debt + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
3.3 Risk Management and Insurance					
Employers Liability Insurance Certificate	No	Year of issue + 40 years. Pass to the Local Authority if the school closes		SECURE DISPOSAL	irms Toolkit for Schools
Insurance policies	No	Date the policy expires + 6 years except Public Liability insurance - day of issue + 40 years		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the settlement of insurance claims	Yes	Date claim settled + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Burglary, theft and vandalism report forms		Current year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Audit Committee and appointment of responsible officers	No	As long as necessary		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
3.4 School Fund					
School Fund Ledger	Yes [ledger may contain names of people in receipt of grants]	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Whole of government accounts returns	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
School Fund Journey books	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
School Fund Invoices	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
School Fund Receipts	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
School Fund Bank statements	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
School Fund Cheque books	No	Current financial year + 1 year		SECURE DISPOSAL	irms Toolkit for Schools
School Fund Paying in books	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
3.5 School Meals					
Free school meals registers	Yes	Current financial year + 3 years		SECURE DISPOSAL	irms Toolkit for Schools
School meals summary sheets	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
School meals registers	Yes	Current financial year + 3 years		SECURE DISPOSAL	irms Toolkit for Schools
3.6 Strategic Finance					
Annual accounts	No	Current year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
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	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Statement of financial activities for the year	No	Current financial year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Financial Planning	No	Current financial year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Value for money statement	No	Current financial year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Borrowing powers	No	Until superseded + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Charging and remissions policy	No	Date policy superseded + 3 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Independent Auditors report on regularity	No	Financial year report relates to + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Independent Auditors report on financial statements	Yes	Financial year report relates to + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the management of VAT	No	Current financial year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
4. Governing Bodies					
4.1 Activities					
Records relating to Governor Monitoring Visits	Yes	Date of the visit + 3 years		SECURE DISPOSAL	irms Toolkit for Schools
4.2 Governance					
Constitution	No	Date constitution superseded + 10 years. It may be appropriate to retain one copy of each constitution for archival purposes	Companies Act 2006 section 355	SECURE DISPOSAL	irms Toolkit for Schools
Articles of Association	No	Life of the Academy		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Memorandum of Association	No	This can be disposed of once the Academy has been incorporated		SECURE DISPOSAL	irms Toolkit for Schools
Memorandum of Understanding of Shared Governance among Schools	No	Life of Memorandum of Understanding + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Governance Statement	No	Life of governance statement + 6 years. One copy of each iteration may need to be retained for archive purposes		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Special Resolutions to amend the Constitution	No	Date constitution superseded + 10 years. It may be appropriate to retain one copy of each constitution for archival purposes	Companies Act 2006 section 355	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Annual Report and Accounts	No	Date of report + 10 years	Companies Act 2006 section 355	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Annual Report Trustees Report	No	Date of report + 10 years	Companies Act 2006 section 355	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Annual Reports created under the requirements of the Education (Governors Annual Reports) (England) (Amendment) Regulations 2002	No	Date of report + 10 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Annual Return	No	Date of report + 10 years	Companies Act 2006 section 355	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Instruments of Government	No	For the life of the school		Consult local archives before disposal	irms Toolkit for Schools
Register of Directors	Yes	Date Director resigns + 10 years Companies Act Section121 Removal of entries relating to former members. An entry relating to a former member of the company may be removed from the register after the expiration of ten years from the date on which he ceased to be a member	Companies Act 2006 section 355	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Scheme of Delegation and Terms of Reference for Committees	No	Until superseded or whilst relevant [Schools may wish to retain these records for reference purposes in case decisions need to be justified]		These could be offered to the archives if appropriate	irms Toolkit for Schools
Trusts and Endowments managed by the Governing Body	Yes	Life of the Trust or Endowment + 6 years		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Records relating to complaints dealt with by the Governing BodyAnnual Report and Accounts	Yes	Date complaint resolved + 3 years then review. If the complaint relates to negligence or safeguarding then date the complaint resolved + 15 years. If the complaint relates to child sexual abuse then the complaint resolved + 75 years (this retention period will be reviewed once the government and the ICO have issued guidance about the implementation of the IICSA recommendations)		SECURE DISPOSAL	irms Toolkit for Schools
All records relating to the conversion of schools to Academy status	No	For the life of the organisation	Companies Act 2006 section 355	Consult local archives before disposal	irms Toolkit for Schools
Policy documents created and administered by the Governing Body	No	Until superseded. The School should consider keeping all policies relating to safeguarding, child protection or other pupil related issues such as exclusion until the government and ICO have published guidance about the implementation of the recommendations made in the IICSA report		SECURE DISPOSAL	irms Toolkit for Schools
4.3 Governors, Directors and Trustees					
Appointment of Trustees and Governors and Directors	Yes	Life of appointment + 6 years	Companies Act 2006 section 355	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the election of parent and staff governors not appointed by the governors	Yes	Date of election + 6 months		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the appointment of co-opted governors	Yes	Provided that the decision has been recorded in the minutes the records relating to the appointment can be destroyed once the co-opted governor has finished their term of office except where there have been allegations concerning children. In this case retain for 25 years.		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the terms of office of serving governors including evidence of appointment	Yes	Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years.		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to Governor Declaration against disqualification criteria	Yes	Date appointment ceases plus 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Governors Code of Conduct	No	This is expected to be a dynamic document, one copy of each version should be kept for the life of the organisation		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Records relating to DBS checks carried out on clerk and members of the governing body	Yes	Date of DBS check + 6 months (but need to retain a record of the date of the DBS check if you are renewing every 3-5 years depending on policy)		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Governor personnel files	Yes	Date appointment ceases plus 6 years except where there have been allegations concerning children. In this case retain for 25 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the induction programme for new governors	Yes	Date appointment ceases plus 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the training required and received by Governors	Yes	Date Governor steps down + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Appointment and removal of Members	No	Life of appointment + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Register of members		Date Member resigns + 10 years	Companies Act 2006	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Statement of Trustees Responsibilities	No	Life of statement + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Register of Trustees interests	Yes	Date Trustee resigns + 10 years	Companies Act 2006	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Declaration of Interests Statements [Governors] [this is not a statutory register]	Yes	Date Governor resigns + 10 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
4.4 Meetings					
Board Meeting Minutes	Yes	Minutes must be kept for at least 10 years from the date of the meeting	Companies Act 2006 section 248	OFFER TO ARCHIVES	DfE Data Protection in Schools, irms Toolkit for Schools
Board Decisions	Could be if the decisions refer to living individuals	Date of the meeting + a minimum of 10 years		OFFER TO ARCHIVES	DfE Data Protection in Schools, irms Toolkit for Schools
Board Meeting: Annual Schedule of Business	No	Current year		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Board Meeting: Procedures for conduct of meeting	No	Date procedures superseded + 6 years	Limitation Act 1980 (Section 2)	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the management of General Members Meetings	No	Minutes must be kept for at least 10 years from the date of the meeting	Companies Act 2006 section 248	OFFER TO ARCHIVES	DfE Data Protection in Schools, irms Toolkit for Schools
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	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to the management of the Annual General Meeting	Could be if the minutes refer to living individuals	Minutes must be kept for at least 10 years from the date of the meeting	Companies Act 2006 section 248	OFFER TO ARCHIVES	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Meetings Schedule	No	Current year		STANDARD DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Agendas 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	DfE Data Protection in Schools, irms Toolkit for Schools
Minutes of, and papers considered at, meetings of the Governing Body and its committees: Principal Set (signed)	May be data protection issues, if the meeting is dealing with confidential issues relating to staff	Date of meeting + 10 years		OFFER TO ARCHIVES	DfE Data Protection in Schools, irms Toolkit for Schools
Minutes of, and papers considered at, meetings of the Governing Body and its committees: Inspection Copies	Yes - May have names and personal issues unless redacted	Date of meeting + 10 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Reports presented to the Governing Body	Yes	Date of meeting the report was presented to + 10 years		SECURE DISPOSAL or retain with the signed set of minute	DfE Data Protection in Schools, irms Toolkit for Schools
Reports made to the Governors Meeting which are referred to in the minutes	Potential	Although generally kept for the life of the organisation, the Local Authority is only required to make these available for 10 years from the date of the meeting.	Companies Act 2006	Consult local archives before disposal	DfE Data Protection in Schools, irms Toolkit for Schools
Register of attendance at Full Governing Board meetings	Yes	Date of last meeting in the book + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Papers relating to the management of the Annual Parents Meeting	Yes	Date of meeting + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
4.5 Health & Safety					
Health and Safety policy statements	No	Life of policy + 3 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Health and safety file to show current state of building including all alterations (wiring, plumbing, building works etc) and to be passed on in the case of change of ownership)	No	Pass to new owner on sale or transfer of building			irms Toolkit for Schools
Fire precautions log books	No	Current year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Fire risk assessments	No unless containing Personal Emergency Evacuation plans	Life of the risk assessment + 3 years	Fire Service Order 2005	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Accident reporting: Adults	Yes	Date of last entry in the accident book + 3 years but if there is possibility of negligence allegation then date of incident + 15 years or date of settlement + 6 years	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to accident/injury at work including incident reports	Yes	Date of incident plus 6 years unless the injury is serious - broken limb, more than 3 days in hospital etc then date of incident plus 15 years (Negligence)		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Accident reporting: Children	Yes	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 IRMSTK17.9 Do not keep completed entries in the book. They must be removed and kept in a locked location.	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Control of Substances Hazardous to Health (COSHH)	No	COSHH sheets should be kept whilst the substance is in use + 6 years COSHH policy documents should be kept until the policy is superseded + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR)	Yes	Date of incident + 3 years provided that all records relating to the incident are held on personnel file. See IRMSTK17.5 and IRMSTK17.7	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471 Regulation 12(2)	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Health and Safety risk assessments	No	Life of risk assessment + 3 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Process of monitoring of areas where employees and persons have or are likely to have come into contact with asbestos	Yes	Last action + 40 years	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Process of monitoring of areas where employees and persons are likely to have come into contact with radiation: Dose assessment and recording	No	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination. To keep the records made and maintained or a copy of these records until the person to whom the record relates has or would have attained the age of 75 years but in any event for at least 30 years from when the record was made	The Ionising Radiations Regulation 2017	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
4.6 Liaison with LEA/DfE					
OFSTED reports and papers	No	Life of the report then REVIEW		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Returns made to central government	No	Current year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
School census returns	No	Current year + 5 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Circulars and other information sent from the Local Authority		Operational use		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Circulars and other information sent from central government	No	Operational use		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Attendance returns	Yes	Academic year + 1 year		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Secondary transfer sheets (Primary)	Yes	Academic year + 2 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
4.7 Parent/Teacher Associations					
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	Yes	Current year + 6 years then REVIEW		SECURE DISPOSAL	irms Toolkit for Schools
4.8 Property					
Title deeds of properties belonging to the school	No	These should follow the property, unless the property has been registered with the Land Registry 12 years from end of deed	 Section 2 of the Limitation Act 1980	Transfer to new owner Dispose of records securely	irms Toolkit for Schools DfE Data Protection in Schools
Plans of property belonging to the school, including any alterations. This is also a health and safety requirement and includes rewiring diagrams and additional fire safety features	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		Pass to next owner	irms Toolkit for Schools
Leases of property leased by or to the school	No	Expiry of lease + 6 years		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Business continuity and disaster recovery plans	Yes	These are dynamic documents which should be kept up to date		SECURE DISPOSAL OF OLD PLANS	irms Toolkit for Schools
Records relating to the letting of school premises	No	Current financial year + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
4.9 Pupils /Students					
Pupils Educational Record required by The Education (Pupil Information) (England) Regulations 2005: Primary	Yes	Retain whilst the child remains at the primary school	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437	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 school should discuss with the local authority about where the file should be stored for the remainder of its statutory retention	DfE Data Protection in Schools, irms Toolkit for Schools
Attendance registers	Yes	Every entry in the attendance register must be preserved for a period of 6 years after the date on which the entry was made. Every back up copy of the register is to be preserved for 6 years after the end of the school year to which it relates.	School attendance Guidance for maintained schools, academies, independent schools and local authorities [updated and re-published annually] School Attendance (Pupil Registration) (England) Regulations 2024	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Correspondence relating to any absence (authorised or unauthorised)	Potential	Current academic year + 2 years	Education Act 1996 Section 7	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
4.10 School Admissions					
All records relating to the creation and implementation of the School Admissions Policy	No	Life of the policy + 7 years.	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	irms Toolkit for Schools
Register of admissions	Yes	Every entry in the attendance register must be preserved for a period of 6 years after the date on which the entry was made. Every back up copy of the register is to be preserved for 6 years after the end of the school year to which it relates.	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities. School Attendance (Pupil Registration) (England) Regulations 2024	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	DfE Data Protection in Schools, irms Toolkit for Schools
Admissions if the appeal is unsuccessful	Yes	Resolution of case + 1 year	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	irms Toolkit for Schools
Admissions if the admission is successful	Yes	Date of admission + 1 year	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Proofs of address supplied by parents as part of the admissions process	Yes	Current academic year + 1 year	School Admissions Code Statutory Guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels	SECURE DISPOSAL	irms Toolkit for Schools
Supplementary information form, including additional information such as religion and medical conditions: For successful admissions	Yes	This information should be added to the pupil file		As per pupil file	irms Toolkit for Schools
Supplementary information form, including additional information such as religion and medical conditions: For unsuccessful admissions.	Yes	Until appeals process completed		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the management of exclusions	Yes	Date of birth of the pupil involved + 25 years		SECURE DISPOSAL	irms Toolkit for Schools
4.11 School Assets					
Community School leases for land	No	Date lease expires + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Commercial transfer arrangements	No	Date lease expires + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Transfer of land to the Academy Trust	No	Life of land ownership then transfer to new owner		SECURE DISPOSAL	irms Toolkit for Schools
Transfers of freehold land	No	Life of land ownership then transfer to new owner		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the leasing of shared facilities, such as sports centres	No	End of lease + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Land and building valuations	No	Date valuation superseded + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Disposal of assets	No	Date asset disposed of + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Burglary, theft and vandalism report forms	No	Date of insurance settlement + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Inventories of furniture and equipment	No	Life of equipment + 6 years. Equipment will have write-down value over several years - the time depending on the type of equipment		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
4.12 School Management					
Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils or members of staff	Date of last entry in the book + a minimum of 6 years then REVIEW		These could be of permanent historical value and should be offered to the County Archives Service, if appropriate	irms Toolkit for Schools
Visitor Management Systems (including electronic systems, visitors books and signing in sheets)	Yes	Academic Year + 1 year [Schools may decide to archive one copy]		SECURE DISPOSAL	irms Toolkit for Schools
School Privacy Notice which is sent to parents as part of GDPR compliance	No	Life of the privacy notice/until the privacy notice plus 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Consents relating to school activities as part of GDPR compliance (for example, consent to be sent circulars or mailings)	Yes	Consents should be retained for as long as the consent is relied on.		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the creation and distribution of circulars to staff, parents or pupils	No	Current year + 1 year		STANDARD DISPOSAL - Schools should decide whether items published on the school website are retained as an archive or whether they should be deleted at the same time as the master copy	irms Toolkit for Schools
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	irms Toolkit for Schools
Reports created by the Head Teacher or the Management Team	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	irms Toolkit for Schools
Management of complaints	Yes	Date complaint resolved + 3 years then review. If the complaint relates to negligence or safeguarding then date the complaint resolved + 15 years. If the complaint relates to child sexual abuse then the complaint resolved + 75 years (this retention period will be reviewed once the government and the ICO have issued guidance about the implementation of the IICSA recommendations)		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Newsletters and other items with a short operational use	No	Current year + 1 year		SECURE DISPOSAL - Schools should decide whether items published on the school website are retained as an archive or whether they should be deleted at the same time as the master copy	irms Toolkit for Schools
Records relating to the creation and publication of the school brochure or prospectus	No	Current year + 3 years. Schools should consider archiving one copy for historical reasons		STANDARD DISPOSAL	irms Toolkit for Schools
4.13 Special Educational Needs and Disabilities					
Special Educational Needs files, reviews and Individual Education Plans	Yes	Date of birth of the pupil + 25 years	Limitation Act 1980	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] unless the document is subject to a legal hold then 6 years after legal action ended	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Advice and information provided to parents regarding educational needs	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] unless the document is subject to a legal hold then date legal action ceases + 6 years	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 2	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Accessibility strategy	Yes	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] unless the document is subject to a legal hold then date legal action ceases + 6 years	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 14	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
5. Teachers and Staff					
5.1 Disciplinary					
Disciplinary Proceedings: Oral warning	Yes	Date of warning + 6 months (warning will not be active after this time but will remain on file as a record of what has occurred)			irms Toolkit for Schools, WCC Disciplinary Policy and Procedures
Disciplinary Proceedings: First Written Warning Level 1	Yes	Date of warning + 6 - 12months (warning will not be active after this time but will remain on file as a record of what has occurred)			irms Toolkit for Schools, WCC Disciplinary Policy and Procedures
Disciplinary Proceedings: Final Written Warning Level 2	Yes	Date of warning + 12months – 3 years (warning will not be active after this time but will remain on file as a record of what has occurred)			irms Toolkit for Schools, WCC Disciplinary Policy and Procedures

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
5.2 Teachers and Staff Pay and Pensions					
Records relating to the agreement of pay and conditions	No	Date pay and conditions superseded + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Payroll records	Yes	Date payroll run + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Payroll reports	Yes	Current year + 6 years 3 years from the end of tax year they relate to	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	DfE Data Protection in Schools irms Toolkit for Schools
Payroll awards	Yes	Current year + 6 years 3 years from the end of tax year they relate to		SECURE DISPOSAL	DfE Data Protection in Schools irms Toolkit for Schools
Payroll gross / net weekly or monthly	Yes	Current year + 6 years 3 years from the end of tax year they relate to	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	DfE Data Protection in Schools irms Toolkit for Schools
Maternity pay records	Yes	Current year + 3 years	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Overtime	Yes	Current year + 3 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
National Insurance Schedule of payments	Yes	Current year + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Insurance	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Sickness records	Yes	Whilst worker is employed at your school Current year + 3 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	DfE Data Protection in Schools irms Toolkit for Schools
Pension payroll	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Superannuation adjustments	Yes	Current year + 6 years	Taxes Management Act 1970; Income and Corporation Taxes 1988	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes	From the end of the year in which the accounts were signed for a minimum of 6 years	Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103) Regulation 15	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
5.3 Recruitment					
All records leading up to the appointment of a new Head Teacher	Yes	Length of appointment + 6 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
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	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
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	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
Pre-employment vetting information DBS Checks	Yes	Schools do not have to keep copies of DBS certificates in order to fulfil the duty of maintaining the single central record. When a school chooses to retain a copy, there should be a valid reason for doing so and it should not be kept for longer than six months. When the information is destroyed, it must be done securely. Once a recruitment (or other relevant) decision has been made, we do not keep certificate information (e.g. DBS number) for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits. If the school disposes of the certificate the following information should be retained in line with the DBS Code of Practice: Retain the following after the certificate is destroyed - 1. The date of issue of a disclosure; 2. The name of the subject; 3. The type of the disclosure requested; the position for which the Disclosure was requested; 4. The unique reference number of the Disclosure; 5. The details of the recruitment decision taken.	DBS Update Service Employer Guide June 2014; Keeping Children Safe in Education.2018 (Statutory Guidance from Dept. of Education) Sections 73, 74	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
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	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
Pre-employment vetting information. Evidence proving the right to work in the United Kingdom	Yes	Where possible, these copies of 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	An employers guide to right to work checks [Home Office May 2015] Last updated 27 April 2022	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
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 plus not less than 2 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
5.4 Safeguarding					
Allegation which is child protection in nature against a member of staff, including where the allegation is unfounded	Yes	Until the persons normal retirement age or 10 years from the date of the allegation, whichever is longer, then REVIEW	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 July 2018	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools, KCSiE
5.5 Staff Management					
Staff Personal File, including employment contract and staff training records	Yes	Termination of employment + 6 years	Limitation Act 1980	SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Timesheets	Yes	Current year + 3 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Absence record	Yes	Current year + 3 years		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Sickness Absence Monitoring	Yes	Sickness records are categorised as sensitive data. There is a legal obligation under statutory sickness pay to keep records for sickness monitoring. Sickness records should be kept separate from accident records' (2003) It could be argued that where sickness pay is not paid then current year + 3 years is acceptable whilst if sickness pay is made then it becomes a financial record and current year + 6 years applies. The actual retention may depend on the internal auditors. Most seem to accept current year+ 3 years as being acceptable as this gives them, 'Benefits' and Inland Revenue time to investigate if they need to.		SECURE DISPOSAL	DfE Data Protection in Schools, irms Toolkit for Schools
Annual appraisal/assessment records	Yes	Current year + 3 years		SECURE DISPOSAL	irms Toolkit for Schools
Records relating to the TUPE process	Yes	Date last member of staff transfers or leaves the organisation + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
Training needs analysis	No	Current year + 1 year		SECURE DISPOSAL	irms Toolkit for Schools
Staff Training where the training leads to Continuing Professional Development	Yes	Length of time required by the professional body		SECURE DISPOSAL	irms Toolkit for Schools
Staff Training except where dealing with children, e.g. First Aid or Health and Safety	Yes	This should be retained on the personnel file		SECURE DISPOSAL	irms Toolkit for Schools
Staff Training where the training relates to children (e.g. safeguarding or other child related training)	Yes	Date of the training + 40 years		SECURE DISPOSAL	irms Toolkit for Schools
Professional Development Plans	Yes	Life of the plan or plan superseded + 6 years		SECURE DISPOSAL	irms Toolkit for Schools
5.6 Teaching and Curriculum					
Schemes of Work	No	Current year + 1 year		It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL	

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Timetable	No	Academic year + 1 year		It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL	irms Toolkit for Schools
Class record books	No	Academic year + 1 year		It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL	irms Toolkit for Schools
Mark books	No	Academic year + 1 year		It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL	irms Toolkit for Schools
Record of homework set	No	Academic year + 1 year		It may be appropriate to review these records at the end of each year and allocate a further retention period, or, SECURE DISPOSAL	irms Toolkit for Schools
Pupils work	Yes	Where possible, work should be returned to the pupil at the end of the academic year. If this is not the schools policy, then current year + 1 year		SECURE DISPOSAL	irms Toolkit for Schools
5.7 Welfare					
Family Liaison Officers and Home School Liaison Assistants: Day Books	Yes	Current year + 2 years then review		SECURE DISPOSAL	irms Toolkit for Schools
Family Liaison Officers and Home School Liaison Assistants: Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes	Whilst child is attending school and then destroy		SECURE DISPOSAL	irms Toolkit for Schools
Family Liaison Officers and Home School Liaison Assistants: Referral forms	Yes	While the referral is current		SECURE DISPOSAL	irms Toolkit for Schools
Family Liaison Officers and Home School Liaison Assistants: Contact data sheets	Yes	Current year then review, if contact is no longer active then destroy		SECURE DISPOSAL	irms Toolkit for Schools

Document	Personal Information	Retention Period	Statutory Provisions	Disposal	Good Practice
Family Liaison Officers and Home School Liaison Assistants: Contact database entries	Yes	Current year then review, if contact is no longer active then destroy		SECURE DISPOSAL	irms Toolkit for Schools
Family Liaison Officers and Home School Liaison Assistants: Group Registers	Yes			SECURE DISPOSAL	irms Toolkit for Schools
Accessibility Plan relating to individual pupils	Yes	The plan should be included on the pupil file	Limitation Act 1980	SECURE DISPOSAL	irms Toolkit for Schools
Child protection information held on pupil file	Yes	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	Keeping children safe in education Statutory guidance for schools and colleges 2018; Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018	SECURE DISPOSAL	irms Toolkit for Schools
Child protection information held in separate files	Yes	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	Keeping children safe in education Statutory guidance for schools and colleges 2018; Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018	SECURE DISPOSAL these records MUST be shredded	irms Toolkit for Schools
Correspondence relating to authorised absence	Yes	Current academic year + 2 years	Education Act 1996 Section 7	SECURE DISPOSAL	irms Toolkit for Schools

Template for SAR request

Thank you for your request for more information regarding your child at school. In order for us to collate the relevant information for you please could you complete the subject access report below:

SUBJECT ACCESS REQUEST	
Name of person requesting information:	
Relationship with the school:	*Please select:* *Pupil / parent / employee / governor / volunteer* *Other (please specify):*
Correspondence address:	
Contact number:	
Email address:	
Details of the information requested:	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible.*

The school will supply the requested information within 1 month of the receipt of this form.

Template letter - Letter of acknowledgment of a SAR

Dear …

Subject Access Request – Re:

Thank you for the Subject Access Request regarding …, which was received in school on DD/MM/YY.

We believe you require:

- Any correspondence (i.e., emails and letters), both internal and external.
-

If this is incorrect, please contact me as soon as possible so that we can ensure your request is appropriately responded to.

We are working with our DPO to identify such data as requested and in compliance with the General Data Protection Regulation's we will reply to you on or before DD/MM/YY.

Once all information has been collated in line with your request, we will contact you again, to arrange release of the data to you.

Please note that proof of identification will be required prior to data being released.

Yours sincerely,

Data Protection Officer

Template - Subject Access Request – School Record Log

Name of Requester:	
Name of Individuals data requested:	
Pupil Date of Birth:	
Date SAR received:	
Date SAR Response required (one calendar month from the above date):	
Is the time limit going to be exceeded? **If yes reasons required:**	Yes / No
Identification of requester verified by:	
Form of identification seen:	
Address of Requester verified by:	
Third Party Authorisation obtained on (if applicable)	
Power of Attorney Documentation verified by (if applicable)	
Check if this is an Education Record Request as set out in the Education (pupil information) (England) Regulations 2005 -	Response time for this is 15 school days
Date initial response made:	
Searches carried out:	
Data searched for:	
Date and who carried out the search:	
Documents found	
Redactions required? Y/N	
Personal Data provided to the Requester: Personal Data Location (Paper files, where? or Electronic)	

Personal Data omitted from the response (i.e. redacted or withheld information):	
Reason for omission	
Actions taken after SAR provided relating to Data Subjects data, eg, Data cleansing in line with the retention schedule (if required)	
Actions taken after SAR provided relating to school policies and procedures, lessons learnt etc (if required)	

Data breach report template

DATA BREACH REPORTING FORM

The purpose of this form is to record an appropriate level of investigation into all possible data breaches, including near miss events, and actions taken thereafter. The Data Protection Lead should complete the form and a copy ultimately shared with the Data Protection Officer. You must inform the DPO as soon as the breach is known – the completion of this form should not slow down the notification to the DPO.

Part 1: Overview to be completed by the Data Protection Lead in School.	
Date of Breach	
Type of Breach Data	Breach / Near Miss
Approximate Number of personal data records concerned	
Approximate number of individuals concerned	
Describe the nature and circumstances of the personal data breach: **Type and amount of personal data:**	
Title or name of the documents: **What personal information is included – eg; Name, address, DOB, Bank account details, description of info about an individual?**	
Describe below the likely consequences of the personal data breach	
Actions taken by recipient when they inadvertently received the information (if applicable)	
Actions taken to retrieve Information and respond to the breach: **Has information been retrieved?**	Yes/ No

When?	Date:
Has loss been contained e.g. all emails deleted?	Yes/ No
Breach of procedure/policy by staff member: **Has there been a breach of policy?**	Yes/ No
Has appropriate management action been taken? **Please provide details:**	
Details of notification to affected data subject: **Has a data subject been notified?** **If not, explain why not?**	Yes/ No
Near Miss - What advice has been given to the affected data subject(s)?	
Has a complaint been received from the Data Subject(s)?	Yes/ No
Details of Data Protection training provided:	
Procedure changes to reduce risks of future data loss to mitigate any possible adverse effects:	

Form completed by:

Date completed:

Please forward this form to your Data Protection Officer (DPO)

Template - Part 2 Initial Assessment

(To be completed by the Data Protection Officer)

Type of event:	Data Breach / Near Miss
Date Report Form Received:	
Initial assessment carried out by (who / date):	
Further investigation required?	Yes / No
ICO reportable? If Yes, date reported:	
Not reported to ICO – reasons for this:	
Notifiable to Individual(s)? If yes, date notified:	
If Individuals not notified reasons for this:	

Data Breach report form completed by: DPO