Sophia
HIGH SCHOOL

Data Protection Policy

2026 - 2027

Ownership & Consultation	
Document sponsors (role)	CEO / Director of Education/Director of EYFS
Document authors (name)	Melissa McBride David McCarthy Vanessa Temple - (From Sept 2022 Version). Jennifer Callaway (From Sept 2023 Version) Fernando Darcie (From Aug 2025 Version) Nina Albarado (From Aug 2025 Version)

Version control	
Implementation date	September 2020
Reviewed	September 2021
Reviewed and updated	September 2022
Reviewed and updated	April 2023
Reviewed and Updated	1st September 2023
Reviewed and Updated	26th December 2024
Reviewed and Updated	August 2024
Reviewed and Updated	August 2025 V3
Reviewed and Updated	August 2026
Next Review	August 2027

Data Protection Policy

Introduction

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

Guidance can be found here:
ICO: GDPR GUIDANCE

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

2. Legislation and guidance

This policy meets the requirements of the UK GDPR, the Data Protection Act 2018, and the **Data (Use and Access) Act 2025**. This policy also takes account of the **Data (Use and Access) Act 2025**, which amends, but does not replace, the UK GDPR and the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. ico.org.uk. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Educational Records and Subject Access Rights

Legal Framework for Private Schools

As a private/independent school, we are **not required** under education regulations to provide parents with access to educational records. The Education (Pupil Information) (England) Regulations 2005 only apply to local authority maintained schools and special schools. Independent schools, academies, and free schools are not obliged to respond to requests for access to pupils' educational records under education legislation.

However, we recognise that parents and pupils retain important rights under data protection legislation.

Subject Access Rights Under UK GDPR Legislation

Pupils' Rights: All pupils, regardless of age, have the right under Article 15 of the UK General Data Protection Regulation (UK GDPR) to request access to their personal data held by the school through a Subject Access Request (SAR).

Parental Rights: Parents may submit a Subject Access Request on behalf of their child if the child is not competent to act on their own behalf or has given their consent. If a child is competent, then the overriding consideration should be what is in their best interests.

Competency Assessment: There is no mandatory age limit for when a pupil may be deemed too young to understand their rights. However, the presumption is that by age 12, a child may have sufficient maturity to understand their rights and make an access request themselves.

What Constitutes Personal Data/Educational Records

The definition of 'educational record' has a wide meaning and includes most information about current and past pupils that is processed by or on behalf of a school. It is likely that most of the personal information a school holds about a particular pupil forms part of the pupil's educational record.

This may include:

- Academic achievements and progress records
- Assessment and examination results
- Attendance records
- Behaviour records and sanctions
- Correspondence from teachers and educational professionals
- Reports and references
- Safeguarding and welfare records
- Medical information provided to the school
- SEND support records
- Communications with parents/carers

Information NOT included:

- Information a teacher keeps solely for their own use
- Information about other pupils (subject to redaction requirements)
- Examination scripts created by pupils themselves

Our Approach to Subject Access Requests

Voluntary Provision: Whilst not legally required to provide educational records under education regulations, we will respond to Subject Access Requests under the UK GDPR within **one calendar month** of receiving a valid request.

No Fees: We do not charge fees for Subject Access Requests for educational records or any other personal data.

Identity Verification: We may request identification to verify the identity of the person making the request, particularly for requests made electronically.

Third Party Data: We will redact information relating to other individuals where disclosure would adversely affect their rights and freedoms, except where this would make the information meaningless or where we are legally required to disclose it.

Exemptions and Restrictions

We may withhold information where:

- Disclosure would be likely to cause serious harm to the physical or mental health of the pupil or another person
- The information relates to child protection concerns and disclosure would not be in the child's best interests
- Legal exemptions under the Data Protection Act 2018 apply
- Court orders restrict disclosure

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, face recognition, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Governing Body - Board of Directors

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

5.2 Data Protection officer

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

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

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

Sophia High School's DPO email address: dataprotection@sophiahigh.school.

5.3 Data Protection Coordinator

The Data Protection Coordinator acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

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

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties.

5.5 Transfer of Data Outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.
The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

5.6 Transfer of Data Outside the UK

The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

6. Data protection principles

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

The principles say that personal data must be:

Processed lawfully, fairly and in a transparent manner:

The first principle is that personal data shall be processed fairly, lawfully and transparently. Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individuals whose data you are using. It is also important to be transparent with individuals in relation to what you do with their data. We let individuals know what we are doing with their data in our privacy notices, these are available on our school website.

Collected for specified, explicit and legitimate purposes:

The second principle is that personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.

As a member of staff at Sophia High School, you may be involved in collecting personal data in different ways. This may include data you receive directly from individuals (for example, by completing educational forms) and data you receive from other sources (including, for example, student records and reports from teachers or credit reference agencies for employees).

You must not use the data for your own personal purposes. Personal data which you collect in the course of your employment, or provision of services, should be used strictly as part of carrying out your role at/for Sophia High School and only for the purpose for which it was collected.

Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

The third principle is that personal data shall be adequate, relevant and limited to what is necessary. You should only collect, use, access or analyse personal data to the extent that you need to.

Accurate and, where necessary, kept up to date

The fourth principle is that personal data shall be accurate and, where necessary, up to date. You should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You should take all reasonable steps to destroy or amend inaccurate or out-of- date data.

Kept for no longer than is necessary for the purposes for which it is processed

The fifth principle is that personal data shall be kept for no longer than is necessary.

Data Protection Legislation does not tell us how long is necessary.

Processed in a way that ensures it is appropriately secure

The sixth principle is that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use of personal data and against accidental loss, destruction or damage.

Data Protection Legislation says that we must use "appropriate, technical and organisational measures") to keep data secure. Security of personal data applies to a range of areas, including IT security, and it should be applied throughout your day-to-day activities

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

7. Collecting personal data

Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden). We will only rely on **recognised legitimate interests** as defined under the Data (Use and Access) Act 2025—for example, for public security ico.org.uk —and will document our assessment of the impact on individuals.
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given

clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018. As we are a fully digital school and offer online services to students, such as Google Classroom and associated educational applications, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services). We comply with the **Age Appropriate Design Code** (AADC) when offering online services that may be used by children, ensuring our systems are designed with children's privacy in mind. ico.org.uk.

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

Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

8. Sharing personal data

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

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

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Information may be shared without consent where this is necessary to safeguard or promote the welfare of a child, prevent harm, or comply with statutory safeguarding duties.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

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

9. Subject access requests and other rights of individuals

A subject access request ("SAR") is a written request from an individual to obtain information Sophia High School holds about him or her. This is a statutory right, however, it is not without its complications and it doesn't just mean disclosing every piece of information, because there might be legal reasons to withhold certain information.

The individual issuing a SAR could be a pupil, parent and/or guardian of the pupil, member of staff or member of the public. Not everyone who requests personal data will be entitled to receive it, therefore, it is important we verify an individual's right to receive personal data, particularly where the personal data is not about themselves.

As there are strict time periods for complying with a SAR (1 calendar month from the date of the SAR), it is important that you immediately notify the Data Protection Coordinator, who will then assist with the request accordingly.

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

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

Subject access requests may be made verbally or in writing, including by telephone, email, letter or other communication methods. They should include:

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

The person asking for a subject access request must then send an official designated form **(see Appendix B)** to complete and send back. If staff receive a subject access request, they must immediately forward it to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request.

Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests

When responding to requests, we:

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

When responding to a subject-access request, we will carry out **reasonable and proportionate searches** only. ico.org.uk. This means we will search sources likely to contain relevant information without undertaking exhaustive searches. We will still comply with the one-month statutory deadline (with extensions for complex requests where permitted).

We will not disclose information if it:

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

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

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

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

Other data protection rights of the individual

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

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

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

Once all procedures related to the SAR have been completed and you have received the requested information, if you are not satisfied with the outcome then you may wish to follow our complaints procedure.

REASONABLE AND PROPORTIONATE SHARING OF INFORMATION
(DATA USE AND ACCESS ACT 2025)

When required to share information (via a Subject Access Request), we are required to share what is reasonable and proportionate. Transcripts only of video recordings will be shared.

10. Submit a GDPR Related Complaint:

If you have concerns about how we handle your personal data, we are here to help resolve them quickly and fairly. We process GDPR related complaints under the wider School Complaints Policy which can be viewed via our School Policy page on our website available at https://sophiahigh.school/school-policies/

Under the **Data (Use and Access) Act 2025**, we provide an accessible complaints procedure for data-protection matters. Complaints may be submitted via our online form, by email, telephone or post. We will acknowledge your complaint within **30 days** and respond without undue delay. ico.org.uk.

Use our GDPR Online Complaints E-form to raise any data protection concerns. The form is designed to capture the information we need to investigate your complaint thoroughly.

If you prefer not to use the online form, you may also submit data protection complaints by email to dataprotection@sophiahigh.school or by post to

Sophia High School,
Office 315,
The Engine Room,
Battersea Power Station,
London,
SW11 8BZ

As stated in the Complaints Policy, there is a transparent process for us to follow to allow for a full investigation of your concerns, and we will submit our findings within the required timeframe.

If you remain unsatisfied after this, you may consider contacting the ICO.

- Website: ico.org.uk
- Telephone: 0303 123 1113

10. Right to erasure requests

A right to erasure request is a written request from an individual to erase information Sophia High School holds about them. Like SARs, this is a statutory right but not as straightforward as you might think, and it doesn't just mean deleting every piece of information about the individual because there might be legal reasons to keep certain information.

As with SARs, please make sure that you contact your Data Protection Coordinator immediately before responding to the individual making the request.

Please do not respond to the individual without first consulting your Data Protection Co-Ordinator first

11. Parental requests to see the educational record

In the UK, parents of students at independent schools can request access to their child's data, but it's handled through data protection laws like GDPR rather than specific educational record regulations that apply to state schools. They would make a Subject Access Request (SAR) under UK GDPR.

12. Photographs and videos

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

We will obtain written consent from parents/carers for photographs and videos **See Appendix 5** to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

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

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

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

The school will not use photographs or video recordings of children in a way that would place them at risk of harm. Particular care will be taken where safeguarding concerns, court orders, child protection plans or other welfare considerations apply.

13. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see
- section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)

- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data Retention

Purpose of the Data Retention Guide

In the course of its activities every school creates and receives a large amount of information. Much of this information contains personal data which is in turn subject to the Data Protection Act 2018 (DPA 2018).

Personal data is any information relating to a living individual and would include information on pupils, members of staff and other employees. Data can include internal files, letters, faxes, memoranda and notes, email, computer data and even voicemail, SMS etc.

It is extremely important that data is held for the correct period of time so as to be available for the proper needs of the school. Indeed, some classes of data are required by law or good business practice to be kept for a specified period of time and failure to do so may at best prejudice the position of the school and at worst expose the school or its staff and employees to potential lawsuits and/or fines or even put them in contempt of court. However, keeping all data for an unlimited period of time will not only be impractical but will also expose the school to risk under the DPA. This is because the retention of unnecessary data will create a compliance risk under the DPA as this requires that personal data is:

- Adequate relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary

The excessive storage of data is not only highly obstructive to the smooth operation of the school but will also create a risk of prejudicing some or all of the above data protection principles.

The purpose of this guide is to provide guidelines for the retention, storage and disposal of the data held by the school.

Retention Periods

Except as otherwise indicated in accordance with paragraph 4 below data should be retained for the number of years indicated in the Retention Schedule below.

The school is responsible for the implementation of this guide.

Where it is necessary for a school to retain certain data for a period beyond the period indicated in the schedule, the school will maintain a flagging process to those records which must be retained beyond the specified period. The flagging process employed will be dictated by the records system in use. Unless a flag has been given in respect of specific data then data should be destroyed as soon as practicable after expiry of the specified retention period.

See Appendix C: which outlines various timeframes for the keeping of data

Retention of Data beyond the Retention Period

Where data should be retained indefinitely: -

(1) If you receive notice of any lawsuit, government or regulatory investigation (for instance, health & safety investigations), other legal action, complaint or claim against or involving the school, the school or any member of staff, or employee, or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation complaint or claim, then you should flag all data which may be relevant for preservation in respect of the same. Any data so flagged shall be preserved and shall not be destroyed

(2) If any member of staff or employee becomes aware that any notice has been received by the school of any lawsuit, government or regulatory investigation, other legal action, complaint or claim against or involving Co, the school or any member of staff, employee or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation, complaint or claim, that member of staff or employee should immediately notify the school's Data Coordinator in order that the Co-ordinator can review which data should be [flagged] for extended retention in accordance with this guide. The member of staff or employee must not destroy any data relevant to such action, proceeding, investigation, complaint or claim whether it not it would otherwise fall to be destroyed in accordance with this guide.

(3) If any member of staff or employee is unsure whether any unflagged data is relevant to an action, proceeding, investigation complaint or claim the member of staff or employee should not delete that data and should liaise with the Data Coordinator.

Once data has been flagged all members of staff and employees must preserve and prevent the destruction of any such data (including e-mails and other computer records).

Destruction of such data, even if inadvertent, could seriously prejudice the member of staff or employee and the school and could subject the individual, or the school to substantial criminal and civil liability including fines and other penalties.

Whenever data is flagged the data shall be preserved until the flag is removed. The communication imposing the [flag] shall be stored with the preserved data until that flag is removed, following which the data shall be destroyed as soon as reasonably possible.

Archiving data

In general, once data or documents are no longer "live" they should be moved to archiving as soon as is reasonably possible. Archiving should not be confused with destruction. You need to keep in mind that archived data and documents carry with them on-going obligations and are subject to the requirements of the DPA, for instance, archived data and documents will need to be considered in the event of any subject access request and the archiving system must be kept properly secure.

Data and documents which have been archived should be reviewed against the criteria set out in this guide with a view to destruction after the relevant time period. Ultimately the archival period for data and documents is a matter of balancing costs of holding the data or documentation in archive which is highly unlikely ever to be needed against the general principle that everything else being equal, and it is better to be safe than sorry.

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

A personal data security breach is any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It could be as a result of a cybercrime. Or it could be that you, or someone you know, have accidentally shared personal data with another organisation or person without permission.

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

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

When appropriate, we will report the data breach to the ICO (Information Commissioner's Office) within 72 hours.
https://ico.org.uk/for-organisations/report-a-breach/

18. Audit

18.1 Aims of Data Protection Compliance Audits

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- Quality Assurance, ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- Retention, appropriate weeding and deletion of information.
- Documentation on authorised use of systems, e.g. codes of practice, guidelines, etc.
- Compliance with an individual's rights, such as subject access.
- To assess the level of compliance with the organisation's own data protection system.
- To identify potential gaps and weaknesses in the data protection system.
- To provide information for data protection system review.

18.2 Audit Objectives

When carrying out a Data Protection Audit in any area of an organisation the Auditor has three clear objectives:

1. To verify that there is a formal (i.e. documented and up-to-date) data protection system in place in the area.
2. To verify that all the staff in the area involved in data protection:
    - Are aware of the existence of the data protection system;
    - Understand the data protection system;
    - Use the data protection system.

3. To verify that the data protection system in the area actually works and is effective.

18.3 Areas to be examined include:

- Use of appropriate forms when collecting data.
- Storage of data in accordance with the security policy, e.g. locked cabinets, passwords, etc.
- Data being removed in accordance with policy timescales.
- Subject Access Request process in place.
- Staff training requirements assessed and highlighted

See Appendix D – for example of Audit Carried out.

19 Training

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

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

See Appendix E for Teacher Top Tips and Taking data off site.

20. Monitoring arrangements

The DPO/ CIO and the Board of Directors are responsible for monitoring and reviewing this policy.

Appendix A: Personal data breach procedure

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

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

1. The DPO will alert the Director of Education and the Chair of Governors.
2. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
3. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
4. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identity theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's admin server.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach

A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals
- – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on the school's admin server.

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

Actions to minimise the impact of data breaches

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

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant
- unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Sensitive information being disclosed via school website

Member of staff who discovers the sensitive information to inform the DPO as soon as possible.

DPO and tech team to arrange for information to be removed from the school website immediately.

Parents are informed that sensitive information was available on the website and that action has been taken to remove it.

Appendix B: Subject Access Request Template

We provide a template for individuals wishing to submit a Subject Access Request (SAR) which can be found below. Alternatively a SAR request can be made in any format including email or telephone request. Please refer to the template for the information we will need to process your request.

You can also submit your SAR digitally by completing our online form at: https://forms.gle/vTY6dwMVCATiZeHD7.

Request for information under the Data Protection Act 2018

This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type. ***(* Required Fields)***

1. Personal details of the person requesting the information.

Surname:	
Forename:	
Address:	
Postcode:	
Telephone number:	
Email:	

2. Are you the Data Subject ***(i.e. the person whose information you are requesting)?*** Please tick the appropriate box.

Yes □ *(Please go straight to question 5)*

No □

3. **Personal details of the Data Subject** ***(if different from those at section 1).***

Surname:	
Forename:	
Address:	
Postcode:	
Date of birth:	
School attended:	
Telephone number:	
Email:	

4. Please describe your relationship with the Data Subject that leads you to make this request on their behalf.

5. Information requested

If you would like to see only specific document(s), please describe these below.

5. If you would like a full copy of the personal records held by the school, please tick here □.

Declaration

I certify that the information given in this application form to the school is true. I understand that it will be necessary for the school to confirm my/the Data Subject's identity and it may be necessary to supply more detailed information if required.

Signature (Parental Responsibility)

Print Name

Date

Signature (Pupil 12+)

The completed form should be returned to:

The Data Protection Coordinator, Sophia High School, The Engine Room, Battersea Power Station, 18 Power Station Road, London, SW11 8BZ

I understand that I will receive acknowledgement of my request within 5 days of receipt. My request will be completed within one month of the request being received, in normal circumstances in accordance with the DP Act. However please note that Sophia High School will endeavour to complete your request as soon as is practical within this one month period.

Office use only

Received by:	Date:

Forwarded to:	Date:
Date to be completed by:	
Comments:	

Appendix C: Data Retention Schedule

1. Child Protection			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
1.1 Child Protection files	GDPR, DPA 2018, Education Act 2002, s175, related guidance "Keeping Children Safe in Education" (KCSIE)	D.O.B. +25 years Child protection records will be transferred securely when a pupil moves school in accordance with safeguarding guidance.	SECURE DISPOSAL unless legal action is pending
1.2 Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.	GDPR, DPA 2018, Employment Practices Code: Supplementary Guidance 2.13.1. (Records of Disciplinary and Grievance), DfE guidance "Managing Allegations Against Staff" (current version)	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.1 Records related to the formulation of HR Policies and an Employee Handbook	GDPR, DPA 2018	Permanent. Superseded versions: 7 years after being superseded.	SECURE DISPOSAL unless legal action is pending
2.2 List of all members of staff and employees and dates of employment	GDPR, DPA 2018	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.3 Employee offer letters, confirmation of employment letters, written particulars of employment, contracts of employment and changes to	GDPR, DPA 2018	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending

the terms and conditions			
2.4 Information on benefits per member of staff/employee	GDPR, DPA 2018	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.5 Pension records	GDPR, DPA 2018, relevant pension scheme regulations	7 years after termination of employment, or longer as required by specific pension scheme regulations.	SECURE DISPOSAL unless legal action is pending
2.6 Training records	GDPR, DPA 2018	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.7 Collective workforce agreements and works council minutes	GDPR, DPA 2018	Indefinite for current/active agreements; 7 years after expiry/supersession for historical versions.	SECURE DISPOSAL unless legal action is pending
2.8 Job applications, CVs and interview records	GDPR, DPA 2018, The Information Commissioner's Employment Practices Code, Parts 1.7.5 and 1.7.6	6-12 months after notifying unsuccessful candidates; 7 years after termination of an employee if the applicant is hired	SECURE DISPOSAL unless legal action is pending
2.9 Personnel Files (including all records relating to promotions, demotions, grievance procedures, resignation or termination letters)	GDPR, DPA 2018	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.10 Disciplinary Matters			
2.10.1 Verbal Warning	GDPR, DPA 2018, Employment Relations Act 1999	Records resulting from a verbal warning should be retained on file for 6 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.10.2 Written Warning	GDPR, DPA 2018, Employment Relations Act 1999	Records resulting from a written warning should be retained on file for 12 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.10.3 Final Written Warning	GDPR, DPA 2018, Employment Relations Act 1999	Records resulting from a final written warning should be retained on file for 12 months then destroyed.	SECURE DISPOSAL unless legal action is pending
2.11 Job descriptions and performance goals	GDPR, DPA 2018	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending

2.12 Immigration checks	GDPR, DPA 2018, Immigration, Asylum and Nationality Act 2006	Up to 2 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.13 Records in relation to hours worked and payments made to workers	GDPR, DPA 2018, Section 9, National Minimum Wage Act 1998 Regulation 38, National Minimum Wage Regulations 1999	3 years beginning with the day upon which the pay reference period immediately following that which they relate ends	SECURE DISPOSAL unless legal action is pending
2.14 Records relating to accidents / injury at work.	GDPR, DPA 2018, Health and Safety at Work etc. Act 1974, Limitation Act 1980	Date of incident +40 years	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.15 Information relating to the member of staff's/employee's exposure to toxic substances (Medical Records to be stored separately in a confidential location.)	GDPR, DPA 2018	Permanently	SECURE DISPOSAL unless legal action is pending
2.16 Working time opt-out forms	GDPR, DPA 2018, Regulations 5 and 9, Working Time Regulations 1998	2 years from the date on which they were entered into.	SECURE DISPOSAL unless legal action is pending
2.17 Records to show compliance with the Working Time Regulations 1998	GDPR, DPA 2018, Regulations 5, 7 and 9, Working Time Regulations 1998	2 years after the relevant period.	SECURE DISPOSAL unless legal action is pending
2.18 Annual leave records	GDPR, DPA 2018	6 years or possibly longer if leave can be carried over from year to year.	SECURE DISPOSAL unless legal action is pending
2.19 Payroll and wage records for companies	GDPR, DPA 2018, HMRC requirements	6 years from the financial year end in which payments were made.	SECURE DISPOSAL unless legal action is pending
2.20 Maternity records	GDPR, DPA 2018,Regulation 26, Statutory Maternity Pay (General) Regulations 1986	3 years after the end of the tax year in which the maternity pay period ends.	SECURE DISPOSAL unless legal action is pending

2.21 Current bank details	GDPR, DPA 2018	Immediately after use for payroll, or upon termination of employment, unless required for ongoing payment purposes.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.22 Records of advances for season tickets and loans	GDPR, DPA 2018, Limitation Act 1980	While employment continues and up to 6 years after repayment.	SECURE DISPOSAL unless legal action is pending
2.23 Death benefit nomination and revocation forms	GDPR, DPA 2018	While employment continues or up to 6 years after payment of benefit.	SECURE DISPOSAL unless legal action is pending
2.24 Consents for the processing of personal and sensitive data	GDPR, DPA 2018	For as long as the data is being processed and up to 6 years afterwards	SECURE DISPOSAL unless legal action is pending
2.25 Disclosure and Barring Service checks and disclosures of criminal record forms	GDPR, DPA 2018, Rehabilitation of Offenders Act 1974 The Information Commissioner's Employment Practices Code, Parts 1.7.4 and 2.15.3	Should be deleted or securely disposed of within 6 months of issue, following recruitment or the decision not to recruit, unless exceptional, documented reasons for retention. A record of the DBS check (e.g., date, reference number, outcome) may be retained on the personnel file.	SECURE DISPOSAL unless legal action is pending
2.26 Emails - School based staff	GDPR, DPA 2018. Retention dependent on content and purpose (e.g., finance, safeguarding, contractual).	Varies by content; general communications: 6 months after a member of staff leaves employment. Critical content (e.g., contracts, safeguarding reports): Align with the retention period of the related record.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.27 Emails - Head Office staff	GDPR, DPA 2018. Retention dependent on content and purpose (e.g., finance, safeguarding, contractual).	Varies by content; general communications: 10 years after a member of staff leaves employment. Critical content (e.g., contracts, safeguarding reports): Align with the retention period of the related record.	SECURE DISPOSAL unless legal action is pending
2.28 My Documents	GDPR, DPA 2018	Retention should align with the retention periods of the underlying data within the documents.	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.1 Admission Registers	GDPR, DPA 2018, Education (Pupil Information) (England) Regulations 2005 (as amended)	Date of last entry in the book (or file) +6 years.	SECURE DISPOSAL unless legal action is pending
3.2 Attendance Reports	GDPR, DPA 2018, Education (Pupil Information) (England) Regulations 2005 (as amended)	Date of register + 6 years	SECURE DISPOSAL unless legal action is pending
3.3 Pupil Files Retained in Schools			
3.3.1 Primary	GDPR, DPA 2018	Transfer pupil files to the next school when the child leaves. All data except Alumni to be removed 7 years after pupil has left school	SECURE DISPOSAL unless legal action is pending
3.3.2 Secondary	GDPR, DPA 2018, Limitation Act 1980	Until the pupil's 25th birthday	SECURE DISPOSAL unless legal action is pending
3.3.3 Pupil applicants who did not enrol	GDPR, DPA 2018	6-12 months after the end of the academic year for which the application was made.	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.3.4 Special Educational Needs files, reviews and Individual Education Plans	GDPR, DPA 2018, Children and Families Act 2014	D.O.B. + 35 years	SECURE DISPOSAL unless legal action is pending
3.3.5. Records relating to accidents / injury in school	GDPR, DPA 2018, Limitation Act 1980, Health and Safety at Work etc. Act 1974	DOB + 21 years (minimum) or DOB + 25 years (recommended) if the pupil was a minor at the time of the incident	SECURE DISPOSAL unless legal action is pending
3.4 Examination Results			
3.4.1 Internal examination results	GDPR, DPA 2018	7 years after leaving school	SECURE DISPOSAL unless legal action is pending
3.4.2 Any other records created in the course of contact with pupils	GDPR, DPA 2018	7 years after leaving school	SECURE DISPOSAL unless legal action is pending
3.4.3 Statement maintained under the Education Act 1996 section 324.Children and Families Act 2014	GDPR, DPA 2018, Children and Families Act 2014	D.O.B. + 35 years	SECURE DISPOSAL unless legal action is pending
3.5 Proposed statement or amended statement	GDPR, DPA 2018, Children and Families Act 2014	D.O.B. + 35 years	SECURE DISPOSAL unless legal action is pending
3.6 Advice and information for parents regarding Educational needs	GDPR, DPA 2018, Children and Families Act 2014	Closure + 12 years D.O.B. + 35 years, or aligned with the main SEN file if part of that record.	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.7 Accessibility strategy	GDPR, DPA 2018, Special Education Needs Disability Act 2001 section 14.	Closure of strategy period + 12 years	SECURE DISPOSAL unless legal action is pending
3.8Parental permission slips for school trips where there has been a major incident	GDPR, DPA 2018, Limitation Act 1980	D.O.B. of the pupil involved in the incident + 25 years. The permission slips for all pupils on the trips need to be maintained to show that the rules for all pupils had been followed.	SECURE DISPOSAL unless legal action is pending
3.9 Pupil emails	GDPR, DPA 2018. Retention dependent on content and purpose.	Retention should align with the retention periods of the underlying data within the emails. Generic emails may have shorter retention	SECURE DISPOSAL unless legal action is pending
3.10 My Documents	GDPR, DPA 2018.	Retention should align with the retention periods of the underlying data within the documents	SECURE DISPOSAL unless legal action is pending
Curricular records	GDPR, DPA 2018. Specific DfE guidance for assessment data.	Varies by record type (e.g., statutory assessment data may be longer; student work shorter). For statutory assessments, generally 7 years after a pupil leaves school.	SECURE DISPOSAL unless legal action is pending

4. Complaint Records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
4.1 Any data relating to a complaint, issue or potential complaint or issue relating to - any pupil: - the school - any act or omission of any member of staff or other employee or any contractor engaged by the school: - anything which happened in or around any premises occupied by the school	GDPR, DPA 2018	During the period in which the complaint or issue is investigated until final disposition of the matter and thereafter for a period of 7 years .	**DO NOT DESTROY OR DELETE UNLESS AND UNTIL DESTRUCTION HAS BEEN SPECIFICALLY APPROVED BY THE BOARD AND DATA PROTECTION OFFICER** Please refer to IHS Complaints Procedure Policy
4.2 Other e-mail any attachments and voice recording (**unless** other provisions of this guide apply requiring longer retention)	GDPR, DPA 2018	For the period of 2 years	Note : Subject to any, longer retention period which may be required under other provisions of this guide

5. Litigation			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**

5.1 Records relating to pending, threatened or reasonably anticipated litigation, government investigation, or complaint or other claim	GDPR, DPA 2018, Limitation Act 1980	During the period in which the litigation, investigation, complaint or claim is contemplated, pending or threatened and until final disposition of the matter and thereafter for a period of 7 years .	**CHECK WITH THE BOARD AND DATA PROTECTION OFFICER BEFORE DESTROYING** SECURE DISPOSAL unless legal action is pending

Appendix D: Data Protection Audit Return

Data Protection Audit Return

School / Site Name: Year:

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.0	**Staff / Pupil Records**					
1.1	Student data is kept in accordance with the data retention policy.					
1.2	Staff data is kept in accordance with the data retention policy.					
1.3	Expired records are disposed of safely and securely by named individuals.					
1.4	All forms used to collect data are identified.					
1.5	All forms used to collect data include the standard Data Protection disclaimer.					
1.6	The Pupil Data Collection sheet is sent out to parents, annually at a set time, to collect/refresh pupil data.					
1.7	All electronic databases in use, including the users who can access them, are identified.					
1.8	Access to all electronic databases is secured by individual username and password.					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.9	All paper record systems in use, for staff or pupils, are identified.					
1.10	All paper record systems are secured in according to policy guidelines.					
1.11	Staff with access to staff records is documented, controlled and regularly reviewed.					
1.12	The standard Parent Contract is being used.					
1.13	The Accident Book is used for pupils and records are kept for 40 years from the date the incident is logged.					
1.14	The Accident Book is used for staff and records are kept for 40 years from the date the incident is logged.					
1.15	All pupils, whose parents have opted not to have their photograph used, are clearly identified with the information easily accessible to staff.					
2.0	**Procedures**					
2.1	All third-party organisations offering a service on your premises, including the data they collect (if any), are identified. Are any 3rd party provider using Cloud based services, if so please confirm you have discussed this with the Head of IT as indicated in the policy.					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
2.2	All Service Level Agreements with third party organisations are reviewed to consider data handling compliance.					
2.3	All CCTV systems installed at your premises (if any) are documented.					
2.4	Appropriate CCTV signage is in place?					
2.5	The CCTV checklist is completed annually and returned to the Data Protection Officer					
2.6	The school has a policy in place regarding the use of photography/video by family members at events. The method and frequency of communicating this to parents is documented and completed.					
2.7	Contact details of parents are not distributed to other parents, for legitimate school activities, unless signed Parent Consent Form is received by the school (Appendix L).					
2.8	A Subject Access Request (SAR) file is in place to store requests.					
2.9	The SAR process has been tested. Please complete Appendix K1 for a random pupil to test the process and outline any issues or concerns.					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
3.0	**Staff Training**					
3.1	Staff are made aware of the school's Data Protection policy and its implications for them in their work.					
3.2	Staff are made aware of the school's ICT policy, mobile devices and social networking sites policy and its implications for them in their work.					
3.3	Staff are made aware of that they must inform the school of any changes to their personal details, e.g. change of address, contact numbers.					

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
3.4	Have you received staff DP training materials?					
3.5	Have all staff had the minimum training session and been given the DO & DON'T LIST? If not, when is this planned? (*Expectation is that all staff will have been trained by Christmas 2014).*					

Status Key:

Status	Description
	Policy standard not met.
	Policy standard partially met. Action Plan in place to achieve full compliance.
	Policy standard achieved.

Audit completed by (please print):

Signed:

Position:

Date:

Appendix E: TOP TIPS FOR TEACHERS

Here is a list of 'top tips' when handling school data.

DO

- Record facts and professional opinions only, on school records, emails and other similar documents
- Use a strong password on I.T. Systems at work, e.g. a combination of 8 or more alphanumeric characters and symbols.
- Change passwords on a regular basis.
- Password protect email attachments containing personal or commercially sensitive data.
- Encrypt any removable data devices including USB sticks, laptops and similar.
- Remember the school may incur substantial fines for loss or misuse of data.
- Keep data secure when using it off site.
- Think security when posting sensitive documents.

DON'T

- Use personal social media with pupils.
- Contact pupils or store pupil/parent contact data on personal devices, e.g. numbers on your mobile.
- Don't share passwords.
- Don't leave personal data unattended when off site.
- Don't create databases of Personal Data in addition to the official sources e.g. ATHENA / Google Drive / Classroom

Taking Data Off Site

- Only take offsite, information you are authorised to and only when it is necessary.
- ensure that it is protected offsite by not leaving it unattended,
- locking it away when not in use,
- not discussing or sharing it with non-school staff.
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any online services you have used e.g. email
- try to avoid other people seeing the information you are working with
- treat records as if they were your bank details and PIN.