



HARRODIAN

Student, Pupil and Parent Privacy Policy

Contents

1. Aims.....	3
2. Scope.....	3
3. Legislation and guidance.....	3
4. Definitions.....	3
5. The Data Controller.....	4
6. Roles and responsibilities.....	5
7. Data protection principles.....	6
8. Collecting personal data.....	6
9. Sharing personal data.....	7
10. Confirming the identification of individuals.....	7
11. Subject access requests and other rights of individuals.....	8
12. Photographs and videos.....	11
13. Social Media.....	11
14. Processing of Pupil/Student Applications.....	12
15. Bursary.....	12
16. Educational references.....	13
17. CCTV.....	13
18. Peri Services.....	13
19. Visitors.....	14
20. Data protection by design and default.....	14
21. Data security and storage of records.....	15
22. Disposal of records.....	16

23. Personal data breaches.....	16
24. Training.....	16
Appendix 1: Personal data breach procedure.....	18
Appendix 2: Staff Responsibilities.....	21
Appendix 3: Taking data off-site register.....	22
Appendix 4: Data Breach Log.....	23

1. Aims

Our School aims to ensure that all personal data collected about pupils, parents, permanent staff, temporary staff, peripatetic staff, contractors, volunteers, educational advisors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018).

2. Scope

This policy applies to all personal data, regardless of whether it is in paper or electronic format. It encompasses the data required to support the business of Harrodian now and in the future. Although under a single data controller, this policy refers to Harrodian only. Merlin School has its own data privacy policies and procedures.

3. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).

4. Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">● Name (including initials)● Identification number● Location data● Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data (Sensitive)	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">● 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

Confidential personal data	<p>Personal data of an adult which carries the risks of identity theft, criminal impersonation, financial fraud and so needs more protection, including an individual's:</p> <ul style="list-style-type: none"> ● National insurance Number (NI) ● Date of birth ● Credit card details ● Bank account details ● Copy of passport ● Copy of birth certificate
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	An 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.
Student/Pupil	<p>On the school role or has ever been on the school role</p> <ul style="list-style-type: none"> ● Current ● Alumni ● Perspective pupils/students ● Associated relatives who are part of the registration and application process

5. The Data Controller

Our School determines the purpose and means of processing the personal data of parents, pupils, staff, peripatetic teachers, 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.

6. Roles and responsibilities

This policy applies to all students, pupils and parents who are registered with the School, on the school roll or as next of kin or authorised by them. Failure to comply with the policy will be in breach of contract and may result in behavioural sanctions on the pupil/student up to and including exclusion.

6.1 Proprietor

The proprietor has overall responsibility for ensuring that our School complies with all relevant data protection obligations.

6.2 School Chief Privacy Officer (CPO)

The Lead Chief Privacy Officer (CPO) for Harroddian and Merlin is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. In the matter of data privacy, the CPO will report to the proprietor.

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

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

Our CPO is Captain Rob Stewart, and is contactable via email gdpr@harroddian.com

6.3 External Privacy Consultant

The School contracts an external Data Privacy Consultant, **Darren Rose DHR Consultancy**, to support the School in our obligations under the Privacy in Electronic Communications Regulations (PECR), General Data Protection Regulations (GDPR) and Data Protection Act 2018 (DPA18), as well as to provide ongoing support including:

- responding to subject access requests;
- managing data breach incidents; and
- assisting in supplier data protection due diligence

6.4 All Pupils and Parents

Students, pupils and parents are responsible for:

- Providing the School with accurate, up-to-date personal data about themselves, their children and any other persons who have authority to act on their behalf.
- Having the permission to provide personal data of any party who is authorised to act on their behalf with the School for the purposes of education of their child.
- Informing the School of any changes to their personal data, such as a change of address.
- Contacting the CPO 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 believe there has been a data breach.

7. 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.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

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

8. Collecting personal data

8.1 Lawfulness, fairness, and transparency

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

The data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering into a contract.

The data needs to be processed so that the School can **comply with a legal obligation**.

The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.

The data needs to be processed so that the School can perform a task **in the public interest**.

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).

If a child is 12 or over and of maturity, **consent** is obtained from the child, not the parent or guardian, prior to the processing of any subject access requests.

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.

If we offer online services to students/pupils, such as classroom apps or web services, and we intend to rely on consent as a basis for processing, and the child is under 13 years old, we will get parental consent (except for online counselling and preventive services). Most classroom apps or web services will be processed via **legitimate interests**.

8.2 Limitation, minimisation and accuracy

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

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

9. 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, if 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.
- Where possible, establish a data sharing agreement with the supplier or contractor, either in the contract or as a stand-alone 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 as laid out in the Government's 'Information Sharing' paper of July 2018.
- Research and statistical purposes, if 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 that affects any of our pupils or staff.

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

10. Confirming the identification of individuals

All requests (including rights requests) will require the confirmation of identity of the requester.

10.1 An individual known to the School

In some cases, the School may disclose or amend personal data on request from an individual who is known to the School, such as a parent, ex pupil etc or whose identity has been confirmed via other means i.e. pupil number etc.

10.2 Verbal request from an external agency

In cases of verbal requests made by a member of the police, HMRC or other local authority or government department, the requester's identity will be confirmed by calling back the organisation, police station, HMRC office etc. on the publicly available number and asking for the requester.

*In certain time sensitive cases, such as in the vital interests of the data subject, the School may disclose personal data upon authorisation of the School Chief Privacy Officer..

10.3 Standard request from a data subject

In cases of a standard request by a data subject, identity may be confirmed via [2] forms of identification from either:

Officially issued documentation

Valid passport, driving licence or Birth certificate.

Or; utility bill such as:

Council Tax, Water or Phone.

Methods of identity confirmation will not exceed the level of personal data held by the individuals.

11. Subject access requests and other rights of individuals

11.1 Subject access requests

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

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

Subject access requests can be accepted in any form including verbally or via social media channels that the School supports. However, we will need to confirm identification prior to fulfilling the request. A request will be processed quicker if submitted in writing, either by letter, email and including:

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

If staff receive a subject access request, they must immediately forward it to the CPO or Data Privacy Coordinator.

11.2 Children and subject access requests

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

Children below the age of 12 are 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 under 12 years old 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.

Children 12 years and over, if regarded as mature enough to understand their rights and the implications of a subject access request, will need to provide their consent to the School to disclose their information to a parent or guardian unless it is not in the ultimate interest of the child.

If a pupil wishes to withhold authorisation it is important that some form of assessment of competence is carried out which would be along the same line as a Gillick assessment, that is...

"the pupil understands the implications of providing or withholding their consent and has not conducted any other action which would demonstrate a lack of competence."

It is important to ensure a paper trail of the conversation is retained to establish competence, i.e. via email, in case of challenge by a parent or guardian.

Once competence is established an email should be sent to the compliance team...

"it is the professional opinion of the school that the pupil is competent to exercise their rights and the school is not aware of any grounds to overrule their wishes and authorise the sharing in their best interests".

11.3 Responding to subject access requests

When responding to requests, we:

- May, if there is a question over confirming their identity, 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 unless it is determined to be unfounded or excessive.
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is part of a confidential reference.
- Has been given, or collected, on the understanding of confidence.
- Is part of management information.
- Contains information on the position of the School in any negotiations with the requester.
- Contains exam scripts and exam marks of unpublished examination results.
- 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 considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or deemed to be malicious 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 refer to the ICO.

11.4 Other data protection rights of the individual

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

- Withdraw their consent to process (noting that this may impede their education) when given, 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 United Kingdom e.g. for access to systems such as Google Suite for Education.
- 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 CPO by email gdpr@harrodian.com. If staff receive such a request, they will immediately forward it to the CPO.

12. Photographs and videos

As part of our School activities, we may take photographs and record images of individuals within our School for certain purposes including:

12.1 Statutory and School purposes

As part of the School's safeguarding and health and safety legal obligations, photographs of staff may be taken and used for certain purposes such as:

- Within School on notice boards to inform staff, students, and parents of the School Headmaster, Heads of Section, Heads of Year, Safeguarding lead and SEND lead.
- Outside of School with external agencies such as Police, Local Authority, or Department of Education for safeguarding purposes.
- Online on our School website to inform parents of the School Headmaster, Heads of Section, Heads of Year, Heads of Department, Safeguarding lead and SEND lead.

12.2 Marketing and promotional purposes

We will seek agreement via the parental consent form prior to using any photographs or videos taken for marketing or promotional materials. This consent will be sought on arrival in the School and change of phase into Seniors. If 12 years old, or over, the child has the right to consent themselves, and parents need to consider the child's consent.

Uses may include:

- School marketing e.g. school marketing publications, school and sport website.
- Use within School newsletters.
- Use on School social media e.g. Instagram and in local media, such as newspapers.

Even though parents may have provided overall consent for their child's image to be included in a specific promotional material format the School will still respect the wishes of the student and withhold the use of the student's image if there is valid reason to do so, on a case-by-case basis.

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

13. Social Media

Our School has a centralised process for the authorisation of social media accounts which is controlled by the Communications Department. A single point of creation, senior leadership oversight by the CPO and image control simplifies management and allows us to uphold your rights.

Consent is obtained and documented from parents for their consent via the parental consent form for consent regarding their child's image.

Even though parents may have provided overall consent for their child's image to be included in a specific promotional material format the School will still respect the wishes of the student and withhold the use of the student's image on a case-by-case basis.

Consent can be withdrawn at any time via Chloe Warren cwarren@harrodian.com.

14. Processing of Pupil/Student Applications

The School will not hold the personal data of an applicant or parent for longer than is necessary for a lawful purpose. For applications **not** progressed to enrolment, this will generally be no more than two years for applications to the Pre-Prep and one year for 8+ and all other applications.

1. **Pre-Prep Applications:** If an application to the Pre-Prep is not progressed to enrolment, the applicant's details will be retained for up to two years. This allows for potential future enrolment consideration or re-application within this time frame.
2. **8+ and Other Applications Years:** For all other applications, including those for 8+, if the application is not progressed to enrolment, the details will be retained for up to one year after the start of the academic year of entry.
3. **Rollover Applications:** Application details from candidates who meet the criteria for entry but were only offered a place on the waitlist will be retained and rolled over for assessment for the next academic year of entry within that phase (i.e. Pre-Prep, Lower Prep, Upper Prep, Senior, or Sixth Form). These details will be stored securely with the admissions team and retained until the applicant's age would exclude them from that phase.
4. **Non-Eligible Applications:** For candidates who do not meet the criteria for entry and were not progressed to the first-round offer or waitlist, or who withdrew or rejected our offer, their details will not be rolled over to the next academic year admissions process and will be securely deleted in accordance with our data retention policy.

14.1 Interviews

Student applications are securely distributed prior to interviews and collected, and will be securely destroyed following the interview process, as per the School data retention schedule.

14.2 Entrance exams

The School will ask pupils entering Prep or Senior sections to sit an 8+ or 11+ entrance exam which is set by the exam board and shared with an external invigilator. Access to these results is to be requested by the exam board, not the School.

Consent for this retention can be withdrawn at any time by contacting Admissions on 020 8 762 6321.

15. Bursary

Parents can email bursary application forms to the Secretary of the Bursary Fund with supporting documentation to the application including bank statements, pension details, benefits and mortgage payments.

Applicants are prompted, as the application and supporting documents will contain confidential personal data, to send the application securely, either via encrypted email or recorded mail.

The application forms and supporting documents from candidates who are successful in their bursary application, but a place is not available, or they do not pass the entrance exam, are stored securely with the School bursar in case they re-apply within that phase (i.e. Pre-Prep, Prep, Senior or Sixth Form).

16. Educational references

Where an ex-student requires an educational reference or other situations where educational history is needed to be proven, the pupil, or parent, will be required to provide prior written notice of the enquiry along with written consent, including signature, to provide the information to the enquiring party. Depending on the nature of the enquiry, a charge may be levied for this service.

Confidential references

Confirmation will be sought from the requesting party on their use of the confidential reference exemption under the Data Protection Act 2018. If the requesting party confirms their intention NOT to use the exemption, then the School reserves the right to refuse the reference request if the School determines that fulfilling the request may be to the detriment of the School.

17. CCTV

There are several closed loop CCTV systems situated around the School (locations omitted for security reasons).

The School follows the Information Commissioner's Office guidance on CCTV and therefore has a CCTV policy to ensure the security of the captured video, documented controls on its access and retention as well as clearly presented signage informing individuals of its presence and contact details should they wish to exercise their rights.

Access to video recordings can be requested at any time via contact with CPO on 020 8748 6117 option 3 or email gdpr@harrodian.com.

The School reserves the right to refuse access to any video clips containing the image(s) of any other person other than the requester or any circumstance which may be detrimental to the School's position i.e. involvement in a civil claim.

Full details of producers are available in the School *CCTV Policy*.

18. Peri Services

i.e. any peripatetic services which the School facilitates, collects/processes payments between the Peri and the parent.

All peripatetic service providers used by the School will have completed a supplier due diligence review and provided evidence of their appropriate technical and organisational measures employed prior to the School sharing any personal data.

All peripatetic service providers have signed a contract containing confirmation of their legal obligations as a Data Processor.

As the relationship between the School and the peripatetic service provider is not a Joint Controller relationship, each will individually fulfil the rights of the data subject upon request.

19. Visitors

19.1 InVentry Visitor Management System

All visitors to the School will report to the main school office and sign into the InVentry system by providing:

- their name
- their email address
- company name/parent/governor
- car registration details
- who they are visiting – visitors will only be accepted with prior approval from a member of staff

The individual will then either be collected, or escorted to the relevant area and (unless they are DDS checked, in which case they are unescorted and wear a purple lanyard) are always supervised to control access to any personal data which may be on display within the School such as medical alert sheets etc.

19.2 Security Office

Lists of prospective pupils are shared with the school security office to enable admission to the School grounds. The personal data provided includes:

- their name
- year group

The security office destroys the visitors list at the end of each day.

20. Data protection by design and default

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

- Appointing a suitably trained CPO, and ensuring they have the necessary resources to fulfil their duties.
- 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.

- 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.
- 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 CPO 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.

21. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not under the control of a member of staff.
- Paper archived records are stored securely within the School and regularly checked against the School data retention schedule.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is unrestricted access.
- Where personal information needs to be taken off site, there must be appropriate levels of protection via encryption and passwords if electronic, or in secure storage otherwise.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff who store personal information on their private devices are expected to follow the same security procedures as for school-owned equipment (see *our Bring your own device (BYOD) policy* for more information).

- No sensitive personal data is to be retained onto private devices and data must be stored on the School cloud systems.
- 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.

Further details of the School data storage procedures can be seen in the *School Data Retention and Destruction* policy.

22. Disposal of records

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

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

**Further details of the School data retention and storage procedures can be seen in the School Data Retention and Destruction policy.*

23. Personal data breaches

The School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach that impacts the right of the individual, we will follow the procedure:

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

- Safeguarding information being made available to an unauthorised person or posted without sufficient protection.
- The theft or loss of a school laptop or portable device containing non-encrypted personal data about pupils.

24. Training

24.1 All staff

All staff are provided with data protection training on a regular basis, including training as part of their induction process, as applicable:

- GDPR Awareness briefing
- GDPR Sentry - Introduction to Data protection
- GDPR Sentry – Data protection for Administrators
- GDPR Sentry – Data protection for Teaching staff
- GDPR Sentry – Data protection for Senior Leaders

24.2 School CPO

The School CPO completed a **Certified GDPR Practitioner Training Course** to enable them to understand the School legal obligations, under the data protection laws, as well as learn the skills and obtain the experience to sufficiently manage and support data protection aspects within the School.

24.3 Senior Leaders, Heads of Year and Heads of Department

Senior members of staff are to complete more detailed GDPR training than the other staff to enable them to sufficiently identify and mitigate risks within their department as well as provide peer support to their team. Data protection also forms part of their continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

24. Monitoring arrangements

The School Chief Privacy Officer is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated, if necessary, as changes are made to the data protection laws that affect our School's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the **full Information Governance Team**.

Document Control:

Reason for version change:	GDPR	Version number:	1.2
Date of Approval:		Approved by:	
Target Audience:	All staff	Date issued:	

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the CPO.

The CPO will investigate the report and determine whether a breach has occurred. To decide, the CPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

The CPO will alert the headteacher and the proprietor.

The CPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).

The CPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

The CPO 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 CPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g. emotional distress), including through:

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

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

The CPO will document the decision (either way) in case it is challenged later by the ICO or an individual affected by the breach. Documented decisions are stored in the School's GDPR Sentry System, accessible through the Seniors Office.

Where the ICO must be notified, the CPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the CPO 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 CPO
- A description of the 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 CPO 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 CPO expects to have further information. The CPO will submit the remaining information as soon as possible.

The CPO 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 CPO 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 CPO
- 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 CPO 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 CPO 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 GDPR Sentry System.

The CPO, Proprietor and Headmaster will 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 CPO as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the CPO will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the CPO 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 CPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The CPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Appendix 2: Staff Responsibilities

All staff and volunteers at our School have a responsibility to ensure data is protected. We will create a data safe environment by doing the following:

- Lock all computers when leaving the screen
- Following all School policies regarding photographs, mobile phones and social networking
- Only taking electronic information off-site where it is encrypted or under two factor authentication
- Ensuring all School electronic devices have a secure password
- Not sending sensitive information via email – members of staff will use encrypted email or password protected documentation if required
- Ensuring all bulk emails are sent using BCC to avoid sharing contact details
- Ensuring the School's internet filtering is used
- Ensuring any personal information is not freely available e.g. on display
- Ensuring any sensitive information is in a locked cupboard
- Ensuring we do not discuss sensitive information with people who do not need to know
- Signing out any physical copies of information we take off site on the register in the School office, and signing it back in
- Disposing of any redundant data securely
- Ensuring all data we own is up to date and accurate
- Reporting any data breaches to the Chief Privacy Officer immediately
- Completing the data breach documentation as soon as possible afterwards
- Teach children about data protection and how to keep their data safe.

Approved by:	Senior Leadership Team
Last reviewed:	July 2024

Updated: July 2024
Date Agreed: July 3rd 2024
Written by: Captain Rob Stewart
Review date: September 2025
Chief Privacy Officer: Captain Rob Stewart

Appendix 3: Taking data off-site register

Date	Data taken	Reason	Time out	Time in	Signed

Appendix 4: Data Breach Log

[illegible]

