



Mary Hare Policy: ORG002

Data Protection Policy

Policy Owner: Data Protection Officer

Date Approved: Autumn 2026

Approved by: Board of Trustees

Next review date: Autumn 2027



Securing the future of deaf children and young people

Contents

1. Policy statement and aims.
 2. Legislation and guidance
 3. Definition of data protection terms
 4. The data controller
 5. Roles and responsibilities
 6. Data protection principles
 7. Collecting personal data (Fair and lawful processing & Notifying data subjects)
 8. Sharing personal data (Disclosure and sharing of personal information)
 9. Subject access requests and other rights of individuals (Processing in line with data subject's rights)
 10. Parental requests to see the educational record.
 11. Biometric recognition systems
 12. CCTV
 13. Photographs and videos (Images and videos)
 14. Artificial intelligence (AI)
 15. Data protection by design and default
 16. Data security and storage of records
 17. Disposal of records
 18. Personal data breaches and procedure
 19. Training
 20. Monitoring arrangements
 21. Links with other policies
- APPENDIX 1: Personal data breach procedure

Executive Summary

The Board of Trustees has overall accountability for data protection compliance. The Data Protection Officer (DPO) provides independent oversight, advice and monitoring, while all staff, trustees, volunteers and third parties acting on behalf of Mary Hare are responsible for handling personal data in accordance with this policy and associated procedures.

Mary Hare's data protection control framework is based on clear accountability, privacy by design, staff training, risk assessment, data security measures, records management, breach reporting procedures, and regular monitoring and review. Data protection considerations must be incorporated into all new projects, systems and processes involving personal data.

Compliance with this policy is essential to maintaining the trust of our pupils, families, staff and wider community, and to ensuring that Mary Hare meets its legal and regulatory obligations.

1. Policy statement and Aims

- 1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities as Mary Hare, we will collect, store and process personal data about our pupils, workforce, parents and others. This makes us a data controller in relation to that personal data.
- 1.2 We are committed to the protection of all personal data and special category personal data for which we are the data controller.
- 1.3 The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied.
- 1.4 All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.
- 1.5 **Aims:** Mary Hare aims to ensure that all personal data collected about staff, pupils, parents and carers, Trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

- 2.1 The types of personal data that we may be required to handle include information about pupils, parents, our workforce, and others that we deal with. The personal data which we hold is subject to certain legal safeguards specified in the **UK General Data Protection Regulation ('UK GDPR')**, which incorporates the EU GDPR with UK amendments, the Data Protection Act 2018, and other regulations (together 'Data Protection Legislation').
- 2.2 This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

- 2.3 This policy is based on guidance published by the **Information Commissioner's Office (ICO)** on the UK GDPR and guidance from the **Department for Education (DfE)** on Generative artificial intelligence in education.
- 2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 2.5 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process personal data.
- 2.6 Mary Hare is a Non-Maintained Special School, and this policy complies with our Articles of Association.
- 2.7 This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.
- 2.8 This policy also reflects the ICO's guidance for the use of surveillance cameras and personal information.

3. Definition of data protection terms

- 3.1 All defined terms in this policy are indicated in bold text, and a list of definitions is included in this section.
 - **Data:** Information, which is stored electronically, on a computer, or in certain paper-based filing systems.
 - **Data Subjects:** For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
 - **Personal Data:** Any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
 - **Data Controllers:** The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
 - **Data Users:** Those of our workforce (including Trustees and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
 - **Data Processors:** Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.

- **Processing:** Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties. Processing can be automated or manual.
- **Special Category Personal Data:** Personal data which is more sensitive and needs more protection. This includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data, where used for identification purposes.
- **Workforce:** Includes any individual employed by Mary Hare such as staff and those who volunteer in any capacity including Trustees/Governors.
- **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

- 4.1 Mary Hare processes personal data relating to parents and carers, pupils, staff, trustees, visitors and others, and therefore is a Data Controller.
- 4.2 Mary Hare is a registered charity (1048386) and is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

- 5.1 This policy applies to all staff employed by Mary Hare, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.
- 5.2 **Trustee Board:** The Trustee Board has overall responsibility for ensuring that Mary Hare complies with all relevant data protection obligations.
- 5.3 **Data Protection Officer (DPO):** Our DPO is Peter Robson (Chief Operating Officer), who can be contacted at dpo@maryhare.org.uk.
 - 5.3.1 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy.
 - 5.3.2 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.
 - 5.3.3 The DPO's role includes overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

5.3.4 The DPO will provide a regular data protection update report directly to the HR & G Committee.

5.3.5 The DPO performs their duties independently to avoid conflicts of interests.

5.4 **CEO/Principal:** The CEO/Principal acts as the representative of the Data Controller on a day-to-day basis.

5.5 **All staff:** Staff are responsible for:

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

6. Data protection principles

6.1 Anyone processing personal data must comply with the data protection principles. These provide that personal data must be:

- Processed **lawfully, fairly and transparently** in relation to the data subject.
- Processed for **specified, lawful purposes** and in a way which is not incompatible with those purposes.
- **Adequate, relevant and not excessive** for the purpose.
- **Accurate and up to date.**
- Not kept for any longer than is necessary for the purpose.
- Processed **securely** using appropriate technical and organisational measures.

6.2 Personal data must also:

- Be processed in line with data subjects' rights.
- Not be transferred to people or organisations situated in other countries without adequate protection.

6.3 We will comply with these principles in relation to any processing of personal data by Mary Hare.

7. Collecting personal data (fair and lawful processing & notifying data subjects)

7.1 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 data subject.

7.2 For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing.
- Whether the personal data will be shared, and if so with whom.
- The period for which the personal data will be held.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

7.3 We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing.

7.4 For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally process personal data under the following legal grounds:

- Where the processing is necessary for the performance of a contract between us and the data subject, such as an employment contract.
- Where the processing is necessary to comply with a legal obligation that we are subject to, (e.g., the Education Act 2011).
- Where the law otherwise allows us to process the personal data or we are carrying out a task in the public interest.
- Where none of the above apply then we will seek the consent of the data subject to the processing of their personal data.

7.5 When special category personal data is being processed then an additional legal ground must apply to that processing. We will normally only process special category personal data under following legal grounds:

- Where the processing is necessary for employment law purposes, for example in relation to sickness absence.
- Where the processing is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment.

- Where the processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities.
- Where none of the above apply then we will seek the consent of the data subject to the processing of their special category personal data.

7.6 **Note on the Data Use and Access Act 2025 (DUAA):** This new legislation, phased in from June 2025, may impact consent and legitimate interests. It aims to help organisations innovate, particularly in scientific research, including commercial scientific research.

The DUAA allows for "**broad consent**" to an area of scientific research, rather than highly specific consent for each project. It also allows re-use of personal information for scientific research without a privacy notice if obtaining one would involve disproportionate effort, provided rights are protected and notice is published on a website.

The Data (Use and Access) Act 2025 introduces recognised legitimate interests in certain circumstances and provides greater flexibility for specific types of processing. The school will review its policies and practices to ensure compliance as relevant DUAA provisions come into force and the ICO issues governance guidance.

Where automated decision-making is used, appropriate safeguards, including opportunities for human review and challenge, will be maintained.

7.7 We will inform data subjects of the above matters by way of appropriate privacy notices which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

7.8 If any data user is in doubt as to whether they can use any personal data for any purpose then they must contact the DPO before doing so.

7.9 **Vital Interests:** There may be circumstances where it is considered necessary to process personal data or special category personal data in order to protect the vital interests of a data subject. This might include medical emergencies where the data subject is not in a position to give consent to the processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

7.10 **Consent:**

7.10.1 Where none of the other bases for processing set out above apply then Mary Hare must seek the consent of the data subject before processing any personal data for any purpose.

7.10.2 There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

7.10.3 When pupils and/or our workforce join Mary Hare, a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, among other things. Where appropriate third parties may also be required to complete a consent form. 7.10.4

7.10.4 In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

7.10.5 Where appropriate consent will be sought directly from a pupil who has reached the age of 12, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

7.10.6 If consent is required for any other processing of personal data of any data subject, then the form of this consent must:

- Inform the data subject of exactly what we intend to do with their personal data.
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in.
- Inform the data subject of how they can withdraw their consent.

7.10.7 Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

7.10.8 The DPO must always be consulted in relation to any consent form before consent is obtained.

7.10.9 A record must always be kept of any consent, including how it was obtained and when.

7.11 **Processing for Limited Purposes:** In the course of our activities as Mary Hare, we may collect and process the personal data set out in our Schedule of Processing Activities. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, local authorities, other Mary Hares, parents, other pupils or members of our workforce). We will only process personal data for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject. 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.

7.12 **Notifying Data Subjects / Privacy Notices:**

7.12.1 If we collect personal data directly from data subjects, we will inform them about:

- Our identity and contact details as data controller and those of the DPO.
- The purpose or purposes and legal basis for which we intend to process that personal data.
- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- Whether the personal data will be transferred outside the United Kingdom and, where applicable, outside countries recognised as providing adequate protection
- The period for which their personal data will be stored, by reference to our Record Retention Policy.

- The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making.
- The rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

7.12.2 Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible, thereafter, informing them of where the personal data was obtained from.

7.12.3 We will ensure that our privacy notices are regularly reviewed and updated to reflect any changes in how personal data is collected, used, or shared.

8. Sharing personal data (Disclosure and sharing of personal information)

8.1 We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- We may share personal data that we hold about data subjects, and without their consent, with other organisations. Such organisations include the Department for Education, Ofsted, health authorities and professionals, the Local Authority, examination bodies, other Mary Hare entities, and other organisations where we have a lawful basis for doing so.
- 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 that can provide sufficient guarantees that they comply with UK data protection law.
 - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.
 - Only share data that the supplier or contractor needs to carry out their service.
- We will also share personal data with law enforcement and government bodies where we are legally required to do so. Mary Hare will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example where personal data is shared with the police in the investigation of a criminal offence.
- 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.

8.2 In some circumstances we will not share safeguarding information. Please refer to our Safeguarding Policy.

8.3 Further detail is provided in our Schedule of Processing Activities.

- 8.4 Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Subject access requests and other rights of individuals (Processing in line with data subject's rights)

- 9.1 We will process all personal data in line with data subjects' rights, in particular their right to:

- Request access to any personal data we hold about them.
- Object to the processing of their personal data, including the right to object to direct marketing.
- Have inaccurate or incomplete personal data about them rectified.
- Restrict processing of their personal data.
- Have personal data we hold about them erased.
- Have their personal data transferred.
- Object to the making of decisions about them by automated means.
- Be notified of a data breach (in certain circumstances).
- Make a complaint to the ICO.

9.2 The Right of Access to Personal Data (Subject Access Requests - SARs)

9.2.1 Data subjects may request access to all personal data we hold about them. Such requests will be considered in line with the Mary Hare's Subject Access Request Procedure.

9.2.2 A Subject Access Request includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

9.2.3 Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include: Name of individual, correspondence address, contact number and email address, and details of the information requested.

9.2.4 If staff receive a subject access request in any form, they must immediately forward it to the DPO.

9.3 Children and Subject Access Requests (SARs):

9.3.1 **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.

9.3.2 For **Mary Hare Primary School pupils (children below the age of 12)**, they 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 Mary Hare may be granted without the express permission of the pupil.

9.3.3 For **Mary Hare Secondary School pupils (children aged 12 and above)**, they are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at Mary Hare may not be granted without the express permission of the pupil.

9.3.4 In all cases, a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.4 Responding to Subject Access Requests: When responding to requests, we:

- We may request reasonable evidence of identity where necessary and may ask the individual to provide up to two 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 (or receipt of the additional information needed to confirm identity, where relevant).
- Will provide the information free of charge.
- May tell the individual we will comply within three 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.
- The school will carry out searches that are reasonable and proportionate when responding to Subject Access Requests. The scope of searches will be determined by the circumstances of the request, the systems likely to contain relevant information, the volume of records involved and the importance of providing access to the personal data requested.
- We may not disclose information for a variety of reasons, such as if it:
 - Might cause serious harm to the physical or mental health of the pupil or another individual.

- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
 - Would include another person's personal data that cannot be reasonably anonymised, and the other person has not given their consent, and it would be unreasonable to proceed without it.
 - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, current on-going internal grievance or disciplinary process, management forecasts, negotiations, confidential references, or exam scripts.
- If the request is unfounded or excessive, Mary Hare may refuse to act on it or charge a reasonable fee to cover administrative costs. Mary Hare will take into account whether the request is repetitive in nature when making this decision.
 - When a request is refused, the individual will be informed why and advised they have the right to complain to the ICO, or they can seek to enforce their subject access right through the courts.
 - Only with the authorisation of the DPO (or in their absence the CEO/Principal), will search tools be used to identify and locate personal data subject to a SAR. These tools may look across all databases including but not limited to email exchange servers, Sharepoint and One Drive servers. Only limited access will be granted to the search tools and any related output to maintain confidentiality.

9.5 **The Right to Object:**

- 9.5.1 In certain circumstances data subjects may object to us processing their personal data. This right may be exercised in relation to processing that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.
- 9.5.2 An objection to processing does not have to be complied with where the Mary Hare can demonstrate compelling legitimate grounds which override the rights of the data subject.
- 9.5.3 Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.
- 9.5.4 In respect of direct marketing any objection to processing must be complied with.
- 9.5.5 Mary Hare is not however obliged to comply with a request where the personal data is required in relation to any claim or legal proceedings.

9.6 **The Right to Rectification:**

- 9.6.1 If a data subject informs us that personal data held about them by Mary Hare is inaccurate or incomplete then we will consider that request and provide a response within one month.
- 9.6.2 If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary, then we will inform the data subject within one month of their request that this is the case.

- 9.6.3 We may determine that any changes proposed by the data subject should not be made. If this is the case, then we will explain to the data subject why this is the case. In those circumstances we will inform the data subject of their right to complain to the Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

9.7 **The Right to Restrict Processing:**

- 9.7.1 Data subjects have a right to 'block' or suppress the processing of personal data. This means that Mary Hare can continue to hold the personal data but not do anything else with it.

- 9.7.2 Mary Hare must restrict the processing of personal data:

- Where it is in the process of considering a request for personal data to be rectified.
- Where Mary Hare is in the process of considering an objection to processing by a data subject.
- Where the processing is unlawful, but the data subject has asked Mary Hare not to delete the personal data.
- Where Mary Hare no longer needs the personal data, but the data subject has asked Mary Hare not to delete the personal data because they need it in relation to a legal claim, including any potential claim against Mary Hare.

- 9.7.3 If Mary Hare has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

- 9.7.4 The DPO must be consulted in relation to requests under this right.

9.8 **The Right to Be Forgotten (Erasure):**

- 9.8.1 Data subjects have a right to have personal data about them held by Mary Hare erased only in the following circumstances:

- Where the personal data is no longer necessary for the purpose for which it was originally collected.
- When a data subject withdraws consent – which will apply only where Mary Hare is relying on the individuals consent to the processing in the first place.
- When a data subject objects to the processing and there is no overriding legitimate interest to continue that processing.
- Where the processing of the personal data is otherwise unlawful.
- When it is necessary to erase the personal data to comply with a legal obligation.

- 9.8.2 Mary Hare is not required to comply with a request by a data subject to erase their personal data if the processing is taking place:

- To exercise the right of freedom of expression or information.
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law.

- For public health purposes in the public interest.
- For archiving purposes in the public interest, research or statistical purposes.
- In relation to a legal claim.

9.8.3 If Mary Hare has shared the relevant personal data with any other organisation, then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

9.8.4 The DPO must be consulted in relation to requests under this right.

9.9 **Right to Data Portability:** In limited circumstances a data subject has a right to receive their personal data in a machine readable format, and to have this transferred to another organisation. If such a request is made, then the DPO must be consulted.

9.10 **Right to Withdraw Consent:** Individuals have the right to withdraw their consent to processing at any time.

10. Parental requests to see the educational record

- 10.1 Mary Hare is a Non-Maintained Special School, and there is no automatic parental right of access to the educational record in this setting. However, Mary Hare chooses to provide parents/carers with access to their child's educational record upon written request.
- 10.2 Requests should be made in writing to the DPO. Requests will be considered alongside applicable data protection safeguarding and confidentiality obligations.
- 10.3 Mary Hare will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant). This period may be extended to three months for complex or numerous requests, with the individual informed within one month of the reason for the delay.
- 10.4 If the request is for a copy of the educational record, Mary Hare may charge a reasonable fee to cover the cost of supplying it.
- 10.5 There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

- 11.1 In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.
- 11.2 Should Mary Hare use workforce or pupils' biometric data as part of an automated biometric recognition system (for example, should fingerprint be used to receive meals from the school kitchen), Mary Hare will comply with the requirements of the Protection of Freedoms Act 2012.
- 11.3 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. Mary Hare will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.
- 11.4 Parents/carers and pupils have the right to choose not to use the Mary Hare's biometric system(s). An alternative means providing accessing the relevant services for those pupils.

- 11.5 Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.
- 11.6 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).
- 11.7 Where workforce or other adults use the Mary Hare's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Workforce and other adults can also withdraw consent at any time, and Mary Hare will delete any relevant data already captured.

12. CCTV

- 12.1 Mary Hare operates a CCTV system.
- 12.2 We use CCTV in various locations around the Mary Hare campus to ensure it remains safe. Mary Hare follows the ICO's guidance for the use of CCTV and comply with data protection principles.
- 12.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras must be clearly visible and accompanied by prominent signs explaining that CCTV is in use.
- 12.4 Any enquiries about the CCTV system should be directed to the DPO.
- 12.5 Please refer to the Mary Hare CCTV Policy HSP019 for more detailed information.

13. Photographs and videos (Images and videos)

- 13.1 Parents and others attending Mary Hare events can take photographs and videos of those events for domestic purposes. Mary Hare does not prohibit this as a matter of policy but does not agree to any such photographs or videos being used for any other purpose, acknowledging that such matters are, for the most part, outside of the ability of Mary Hare to prevent. The school asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos for safeguarding reasons, unless all the relevant parents/carers have agreed to this.
- 13.2 Mary Hare celebrates the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering Mary Hare events or achievements.
- 13.3 Mary Hare will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes. Whenever a pupil begins their attendance at Mary Hare, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.
- 13.4 **For Mary Hare Primary School pupils:** We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.
- 13.5 **For Mary Hare Secondary pupils:** We will obtain written consent from parents/carers, or pupils aged under 18, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be

used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

- 13.6 Where the Mary Hare takes photographs and videos, uses may include:
- On School notice boards and in Mary Hare magazines, brochures, newsletters, etc.
 - Outside of Mary Hare by external agencies such as the Mary Hare photographer, newspapers, campaigns
 - Online on the Mary Hare website or social media pages
- 13.7 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.
- 13.8 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.
- 13.9 The use of images and videos will take account of safeguarding considerations and relevant Department for Education guidance. See our Safeguarding and Child Protection Policy SCH010, IT Policy IT001 and Mobile Phone Policy ORG005 for more information on our use of photographs and videos.

14. Artificial intelligence (AI)

- 14.1 Artificial intelligence (AI) tools are now widespread and easy to access. Mary Hare recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data.
- 14.2 To ensure that personal and sensitive data remains secure, **no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.**
- 14.3 If personal and/or sensitive data is entered into an unauthorised generative AI tool, Mary Hare will **treat this as a data breach** and will follow the personal data breach procedure outlined in Appendix 1.
- 14.4 Where AI systems are used to support decision-making, the school will ensure appropriate human oversight and review. AI-generated outputs will not replace professional judgement, safeguarding responsibilities or statutory decision-making processes.
- 14.5. The school will complete Data Protection Impact Assessments (DPIA) before introducing AI systems that process personal data where required by UK GDPR.
- 14.6 See AI and Acceptable Use Policy ORG008 for more information.

15. Data protection by design and default

- 15.1 Mary Hare takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.
- 15.2 Mary Hare demonstrates accountability by maintaining records of processing activities, reviewing compliance arrangements regularly and being able to evidence how data protection obligations are met. 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.
- Processing only 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.
- The organisation will carry out a Data Protection Impact Assessment (DPIA) where a proposed processing activity is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is designed to identify, assess and minimise data protection risks before processing begins.

A DPIA will typically be required where the organisation introduces new technologies, new software, undertakes large-scale processing of personal data, processes special category or criminal offence data on a large scale, conducts systematic monitoring of individuals, or where any processing is likely to significantly affect individuals' privacy.

Staff must consult with the Data Protection Officer at the earliest stage of any initiative, including introducing new software or applications involving the processing of personal data to determine whether a DPIA is required. Processing activities identified as requiring a DPIA must not commence until the assessment has been completed and any identified risks have been appropriately addressed and approved.

Mary Hare will maintain records of completed DPIAs and review them where there are significant changes to the nature, scope, context, or purpose of the processing activity.

- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our Mary Hare and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices).
 - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

16. Data security and storage of records

- 16.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.
- 16.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.
- 16.3 Passwords and authentication controls shall comply with the school's cyber security standards and Multi-Factor Authentication requirements.
- 16.4 Security procedures include:
 - **Entry controls:** Any unidentifiable person seen on site without a visitor's badge/lanyard should be escorted to reception and asked to follow the signing in procedure.
 - **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.). Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
 - **Methods of disposal:** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
 - **Equipment:** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
 - **Working away from the Mary Hare premises – paper documents:** Where possible the use of paper documents containing personal data away from the premises should be avoided. An electronic alternative (laptop) is preferred. However, there are instances when paper documents are required. In such cases, every effort must be made to avoid loss of such documents. Documents must not be left unsupervised. Where personal information needs to be taken off site, staff must sign it in and out from the Mary Hare office.
 - **Working away from the Mary Hare premises – electronic working:** USB data sticks or drives must not be used to transport personal data. If there is no alternative, an encrypted device can be loaned from the Mary Hare office. Mary Hare laptops will conform to our security policies and are therefore the preferred method of working away from the premises with personal data. Passwords that are at least 10 characters long containing letters and numbers are used to access Mary Hare computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
 - **Personal devices:** Staff, pupils or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for Mary Hare-owned equipment, i.e. antivirus protection, MFA authentication App.
 - **Document printing:** Documents containing personal data must be collected immediately from printers and not left on photocopiers.

- **Due diligence for third parties:** 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.
- Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

17. Disposal of records

- 17.1 The school maintains a Records Retention Schedule which sets out how long different categories of personal data are retained and when they will be securely destroyed
- 17.2 Mary Hare will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required.
- 17.3 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.
- 17.4 Disposal of records whether internally or through external third-party suppliers must be carried out in accordance with the Record Retention Policy ORG007.

18. Personal data breaches and procedure

- 18.1 Mary Hare will make all reasonable endeavours to ensure that there are no personal data breaches.
- 18.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1: Personal Data Breach Procedure.
- 18.3 When required the DPO will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a Mary Hare context may include, but are not limited to:
 - A non-anonymised dataset being published on the Mary Hare website, which shows the exam results of pupils eligible for the pupil premium.
 - Safeguarding information being made available to an unauthorised person.
 - The theft of a Mary Hare laptop containing non-encrypted personal data about pupils.
- 18.4 **Mandatory documentation of every breach**, regardless of reporting to ICO, is required. This record will include the facts, cause, effects, and actions taken to contain it and ensure it does not happen again.

19. Training

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

20. Monitoring arrangements

- 20.1 The DPO is responsible for monitoring and reviewing this policy.
- 20.2 This policy will be reviewed annually and approved by the Board of Trustees.
- 20.3 The Board of Trustees nominates one of its Trustees to regularly engage with the DPO and the Head of IT to facilitate governance oversight over data protection. The nominated Trustee/Governor will be a member of the HR & G Committee and provide updates of their oversight work at meetings.

21. Links with other policies

- 21.1 This data protection policy is linked to our:
 - Safeguarding and Child Protection Policy SCH010
 - Privacy Notices
 - Online safety policy IT002 (In draft)
 - CCTV Policy HSP019
 - IT Policy IT001
 - Mobile Phone Policy ORG005
 - Records Retention Policy ORG007
 - AI Policy ORG008

APPENDIX 1: Personal data breach procedure

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

A. Reporting a Breach or Potential Breach

1. On finding or causing a breach or potential breach, the staff member, trustee or data processor must immediately notify the Data Protection Officer (DPO) by email to dpo@maryhare.org.uk. Staff will be required to complete a data breach reporting form with as much relevant detail as possible.

B. Investigation and containment

2. 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.
3. Staff and Trustees will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
4. If a reportable breach has occurred or it is considered to be likely that is the case, the DPO will alert the CEO/Principal.
5. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers).
6. The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

C. Reporting to the ICO and Affected Individuals

7. The DPO will determine whether the breach must be reported to the ICO, and the individuals affected using the ICO's self-assessment tool.
8. The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the GDPR Sentry system.
9. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Mary Hare's awareness of the breach. As required, the DPO will set out:
 - * A description of the nature of the personal data breach including, where possible:
 - * The categories and approximate number of individuals concerned
 - * The categories and approximate number of personal data records concerned

- * The name and contact details of the DPO
- * A description of the likely consequences of the personal data breach
- * A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

10. If all the above details are not yet known, the DPO will report as much as they can within 72 hours of Mary Hare's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

11. Where Mary Hare is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing, in clear, plain language. This notification will set out:

- * A description, in clear and plain language, of the nature of the personal data breach
- * The name and contact details of the DPO
- * A description of the likely consequences of the personal data breach
- * A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

12. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

D. Documentation and Review

13. 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)

14. Records of all breaches will be stored in the GDPR system.

E. Actions to Minimise the Impact of Data Breaches (Examples) Set out below are steps that may be taken to mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- **Sensitive information being disclosed via email (including safeguarding records):**
 - If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
 - Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT department to attempt to recall it from external recipients and remove it from the Mary Hare's email system (retaining a copy if required as evidence).
 - In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
 - The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
 - The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
 - If safeguarding information is compromised, the DPO will inform the designated safeguarding lead.
- **Other types of breach that Mary Hare might consider actions for include:**
 - Details of pupil premium interventions for named children being published on the Mary Hare website.
 - A Mary Hare laptop containing non-encrypted sensitive personal data being stolen or hacked.
 - Mary Hare's cashless payment provider being hacked and parents' financial details stolen.
 - Hardcopy reports sent to the wrong pupils or families.

APPENDIX TO DATA PROTECTION POLICY

Standard SAR Procedure

1. Request Received

- Request may be verbal or written.
- Log the request on GDPR Sentry and create file.

2. Notify Data Protection Officer (DPO)

- DPO records request in SAR log.
- Acknowledge receipt

3. Verify Identity

- If identity is unclear, request further ID (e.g., photo ID + address).
- If a third party is acting on behalf of the data subject, verify their authority.

4. Confirm Personal Data Held

- Check whether the organisation holds personal data about the requester.
- If no data is held, respond accordingly.

5. Collate Relevant Data

- Gather all personal data from relevant systems and departments.
- Ensure completeness and accuracy.

6. Check for Exemptions

- Determine whether any exemptions apply.
- For safeguarding, assess risk of harm before disclosure.

7. Prepare Response

- Collate data in one PDF document.
- Redact data.
- DPO to review and sign off.

8. Issue Response

- Provide the data subject with the information securely
- Must be completed within **one month**, unless an extension appropriate under ICO guidelines.

9. Update SAR Log

- Record decisions, exemptions applied, and date of response.
- File SAR in MH GDPR compliance records.

Subject Access Request Procedure

