Data Protection Policy

Date of last review:	September 2026	**Author:**	EMLM
Date of next review:	September 2027	**Owner:**	EMLM
Type of policy:	☒ Company-wide ☐ Tailored by unit	**Approval:**	Independent Executive Board
Key Contact Email:	info@emlm.org.uk		

Table of Contents

1. Aims 3
2. Legislation and Guidance 3
3. Definitions 3
4. The Data Controller 4
5. Roles and Responsibilities 4
6. Data Protection Principles 5
7. Lawful Processing of Personal Data 6
8. Special Category and Criminal Offence Data 6
9. Children's and Learners' Personal Data 6
10. SEND, EHCP, Health and Safeguarding Information 7
11. Privacy Notices and Transparency 7
12. Sharing Personal Data 7
13. Subject Access Requests 8
14. Requests Concerning Children's Information 8
15. Other Information Rights 9
16. Automated Decision-Making and Profiling 9
17. Artificial Intelligence 9
18. Photographs and Videos 10
19. CCTV 10
20. Biometric Data 10
21. Data Protection by Design and Default 11
22. Data Protection Impact Assessments 11
23. Educational Technology and Third-Party Systems 11
24. Data Security 12
25. Records Retention and Disposal 12
26. International Data Transfers 12
27. Personal Data Breaches 13
28. Data Protection Complaints 13
29. Training and Awareness 13
30. Monitoring and Review 14

Appendix 1 – Personal Data Breach Procedure 15

1. Aims

EMLM is committed to protecting the privacy and personal information of its learners, parents and carers, staff, governors, visitors and all other individuals whose personal data it processes.

EMLM aims to ensure that personal data is collected, used, shared, stored, retained and disposed of lawfully, fairly, transparently and securely.

Given the nature of EMLM's provision, the School may process significant amounts of sensitive information relating to learners, including information about special educational needs and disabilities (SEND), Education, Health and Care Plans (EHCPs), health, behaviour, safeguarding, risk assessments and support needs. EMLM recognises the particular importance of protecting this information.

This policy applies to personal data in any format, including:

- Electronic records;
- Paper records;
- Photographs and video;
- CCTV recordings;
- Emails and electronic communications;
- Information held within school management and safeguarding systems; and
- Information processed through approved third-party systems and services.

2. Legislation and Guidance

EMLM processes personal data in accordance with applicable UK data protection legislation, including:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018;
- The Data (Use and Access) Act 2025 (DUAA);
- The Privacy and Electronic Communications Regulations 2003, where applicable; and
- Other legislation governing the collection, sharing, retention or disclosure of information relevant to the School.

EMLM also has regard to relevant guidance issued by the Information Commissioner's Office (ICO) and, where appropriate to an independent school, Department for Education guidance concerning data protection in education.

The Data (Use and Access) Act 2025 does not replace the UK GDPR or Data Protection Act 2018. It amends and develops the existing data protection framework.

This policy should be read alongside EMLM's:

- Privacy Notices;
- Safeguarding and Child Protection Policy;
- Online Safety Policy;
- CCTV Policy;
- Records Retention Schedule;
- Artificial Intelligence Policy or guidance;
- IT and information security procedures;
- Staff Code of Conduct; and
- Other relevant policies and procedures.

3. Definitions

Personal Data
Any information relating to an identified or identifiable living individual. This may include:

- Name;
- Identification numbers;

- Contact details;
- Location data;
- Online identifiers;
- Photographs or video;
- Educational information; and
- Information relating to an individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Special Category Personal Data
Personal data requiring additional protection because of its particularly sensitive nature. This includes information about:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data used for identification;
- Physical or mental health;
- Sex life; and
- Sexual orientation.

Criminal Offence Data
Personal data relating to criminal convictions and offences or related security measures.

Processing
Any operation carried out on personal data, including collecting, recording, organising, storing, altering, retrieving, viewing, sharing, transmitting, restricting, deleting or destroying it.

Processing may be manual or automated.

Data Subject
The identified or identifiable individual to whom personal data relates.

Data Controller
The organisation or person that determines why and how personal data is processed.

EMLM is a data controller in relation to the personal information for which it determines the purposes and means of processing.

Data Processor
An organisation or person that processes personal data on behalf of a data controller.

Personal Data Breach
A breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The Data Controller

EMLM processes personal data relating to learners, parents/carers, staff, governors, applicants, visitors, contractors and other individuals.

EMLM is therefore a data controller in respect of the personal data for which it determines the purposes and means of processing.

EMLM is registered with the Information Commissioner's Office where required and will maintain the appropriate registration and data protection fee arrangements.

5. Roles and Responsibilities

Proprietor and Independent Executive Board

The Proprietor has overall responsibility for ensuring that EMLM has appropriate arrangements in place to comply with its data protection obligations.

The Independent Executive Board provides appropriate oversight and scrutiny of data protection arrangements in accordance with its delegated responsibilities.

Head of School

The Head of School is responsible for supporting the implementation of this policy and ensuring that staff understand and comply with the School's data protection requirements.

Data Protection Officer

The Data Protection Officer (DPO) oversees EMLM's approach to data protection and provides advice, monitoring and challenge where appropriate.

The DPO's responsibilities include:

- Advising EMLM on its data protection obligations;
- Monitoring compliance;
- Advising on Data Protection Impact Assessments;
- Supporting the management of data breaches;
- Supporting the handling of information rights requests;
- Advising on data sharing and data-processing arrangements;
- Monitoring data protection training and awareness;
- Reporting significant data protection matters to the Proprietor and/or Independent Executive Board; and
- Acting as a contact point with the ICO where appropriate.

EMLM's DPO: Candice Laidley
Email: c.laidley@emlm.org.uk

All Staff

All staff are responsible for protecting personal data they access or process. Staff must:

- Comply with this policy and related procedures;
- Only access personal data required for their role;
- Keep personal information secure and confidential;
- Use School-approved systems for processing personal data;
- Promptly report suspected or actual data breaches;
- Recognise and promptly forward information rights requests to the DPO;
- Not disclose personal data without appropriate authority;
- Complete required data protection training; and
- Seek advice from the DPO where they are unsure about the lawful or secure use of personal information.

Staff must contact the DPO before undertaking new or significantly changed processing that may present a risk to individuals' privacy.

6. Data Protection Principles

EMLM will comply with the principles of data protection law. Personal data must be:

- Processed lawfully, fairly and transparently;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than necessary;
- Processed securely and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

EMLM is also responsible for demonstrating compliance with these principles through appropriate policies, records, procedures and governance arrangements.

7. Lawful Processing of Personal Data

EMLM will identify an appropriate lawful basis before processing personal data. Depending on the circumstances, this may include processing that is necessary:

- For the performance of a contract or to take steps before entering into a contract;
- To comply with a legal obligation;
- To protect someone's vital interests;
- To perform a task in the public interest or exercise official authority, where applicable;
- For EMLM's or a third party's legitimate interests, where those interests are not overridden by the individual's rights and freedoms;
- For a recognised legitimate interest where provided for by legislation; or
- Where the individual has given valid consent.

EMLM will not automatically rely on consent simply because personal information relates to a learner.

Where another lawful basis is more appropriate, such as legal obligation, contractual necessity, safeguarding or another applicable basis, that basis will be used.

Where consent is relied upon, it must be freely given, specific, informed and capable of being withdrawn.

8. Special Category and Criminal Offence Data

EMLM processes special category data only where it has both:

- An appropriate lawful basis under Article 6 UK GDPR; and
- An appropriate condition for processing special category data under Article 9 UK GDPR and, where applicable, the Data Protection Act 2018.

This may include processing relating to:

- Safeguarding and child protection;
- SEND and EHCP provision;
- Physical and mental health;
- Disability and reasonable adjustments;
- Equality monitoring;
- Employment;
- Social protection;
- Substantial public interest;
- Vital interests;
- Health or social care; and
- legal claims.

Where required, EMLM will maintain an Appropriate Policy Document covering relevant processing.

Criminal offence data will only be processed where EMLM has an appropriate lawful basis and legal authority or condition for doing so.

9. Children's and Learners' Personal Data

EMLM recognises that children and young people require particular protection in relation to their personal data.

Information will be presented in a way that is clear and accessible to learners where appropriate to their age, communication needs, capacity and level of understanding. When making decisions concerning a learner's personal data, EMLM will consider:

- The learner's age and maturity;
- Their ability to understand the proposed processing;
- Their communication needs;
- Their SEND;

- Their capacity to make the relevant decision;
- Safeguarding considerations; and
- Their rights and best interests.

A learner's personal data belongs to the learner for data protection purposes. Parental responsibility does not automatically give a parent/carer an unrestricted right to all personal information held about their child.

10. SEND, EHCP, Health and Safeguarding Information

EMLM holds particularly sensitive information about many learners due to the nature of the School's provision. This may include:

- EHCPs;
- SEND assessments;
- Medical and health information;
- Mental health information;
- Medication records;
- Behaviour and incident records;
- Risk assessments;
- Safeguarding and child protection records;
- Information concerning disabilities;
- Professional assessments and reports;
- Information received from local authorities;
- Information received from health and social care professionals; and
- Information relating to support arrangements.

Access to this information will be restricted to those who require it for an appropriate purpose.

Information will only be shared where there is a lawful basis and it is necessary and proportionate to do so.

Data protection law does not prevent EMLM from sharing information where this is necessary and lawful for safeguarding or child protection purposes.

11. Privacy Notices and Transparency

EMLM will provide appropriate privacy information explaining how personal data is used.

Privacy notices will include, as appropriate:

- the identity and contact details of EMLM;
- contact details for the DPO;
- what information is collected;
- why it is processed;
- the lawful basis relied upon;
- who information may be shared with;
- how long information is retained;
- information about international transfers where applicable;
- individuals' data protection rights; and
- how to raise a concern or complaint.

Privacy notices will be reviewed periodically and updated when processing activities or legal requirements change.

12. Sharing Personal Data

EMLM will share personal information where there is a lawful and appropriate reason to do so. This may include sharing information with:

- local authorities;
- education providers;
- examination and awarding organisations;

- health professionals;
- social care;
- safeguarding partners;
- emergency services;
- law enforcement agencies;
- government departments;
- regulatory bodies;
- professional advisers;
- insurers;
- IT and software providers;
- contractors and service providers; and
- other organisations where sharing is lawful and necessary.

Consent is **not always required** before information can lawfully be shared.

In particular, staff must not delay necessary safeguarding information sharing because they believe consent is always required.

Where processors act on EMLM's behalf, the School will undertake appropriate due diligence and ensure suitable contractual data protection provisions are in place.

Only information that is necessary and proportionate for the relevant purpose should be shared.

13. Subject Access Requests

Individuals have the right to request access to personal data EMLM holds about them. A Subject Access Request (SAR) does not have to:

- Be made in writing;
- Use a particular form; or
- Include the words "subject access request".

A request may be made verbally or in writing, including by email or other communication.

All staff must therefore be able to recognise a potential SAR.

Any member of staff receiving a SAR must promptly forward it to the DPO.

EMLM may ask for sufficient information to:

- Verify the requester's identity;
- Establish their authority to act for another person; and
- Reasonably clarify the information being requested where necessary.

EMLM will carry out reasonable and proportionate searches for information within the scope of a request.

The School will normally respond without undue delay and within one calendar month, subject to the provisions in data protection legislation allowing the response period to be paused or extended in particular circumstances.

Where a request is complex, the response period may be extended by up to a further two months where permitted. The requester will be informed of the extension and the reasons for it.

Information will normally be provided free of charge, subject to the circumstances in which legislation permits a reasonable fee or refusal.

Applicable exemptions and the rights of other individuals will be considered before information is disclosed.

14. Requests Concerning Children's Information

The right of access belongs to the child.

A child who has sufficient maturity and understanding to exercise their data protection rights may make a request themselves.

Where a parent/carer makes a request on behalf of a learner, EMLM will consider whether the parent/carer has authority to act on the learner's behalf and whether the learner has sufficient competence and understanding to exercise their own rights.

This will be considered individually rather than determined solely by age. Relevant factors may include:

- The learner's maturity and level of understanding;
- The nature of the information;
- The learner's wishes;
- Family circumstances;
- Safeguarding considerations;
- any court orders or restrictions; and
- whether disclosure would be in accordance with data protection legislation.

Where appropriate, EMLM may seek the learner's views before disclosing information to a parent/carer.

15. Other Information Rights

Subject to the circumstances and applicable exemptions, individuals may have rights to:

- Access their personal data;
- Have inaccurate data corrected;
- Have certain information erased;
- Restrict processing;
- Object to particular processing;
- Withdraw consent where consent is relied upon;
- Data portability in applicable circumstances;
- Receive information about how their data is processed;
- Challenge or seek safeguards in relation to certain automated decisions; and
- Complain about the processing of their personal information.

Requests should be forwarded promptly to the DPO.

16. Automated Decision-Making and Profiling

EMLM will identify where systems involve automated decision-making or profiling.

Where automated processing is used to make a decision producing legal or similarly significant effects on an individual, EMLM will ensure that the processing has an appropriate lawful basis and that applicable safeguards are provided. Where required, these safeguards may include:

- Providing information about the automated processing;
- Enabling the individual to make representations;
- Enabling the individual to obtain meaningful human intervention; and
- Enabling the individual to challenge a decision.

EMLM will undertake a Data Protection Impact Assessment where automated processing is likely to create a high risk to individuals' rights and freedoms.

17. Artificial Intelligence

EMLM recognises that artificial intelligence, including generative AI, can provide educational and administrative benefits but can also create data protection, confidentiality, safeguarding and information-security risks.

Staff and learners must only use AI systems in accordance with EMLM's authorised arrangements and relevant policies.

Personal, confidential, special category or safeguarding information must **not be entered into publicly available or unauthorised AI systems.**

This includes information that could directly or indirectly identify a learner, parent/carer, staff member or other individual.

Before EMLM approves an AI system that will process personal data, consideration will be given to:

- the purpose of processing;
- lawful basis;
- data minimisation;
- security;
- transparency;
- retention;
- supplier terms;
- international data transfers;
- children's rights;
- automated decision-making;
- human oversight; and
- whether a DPIA is required.

Staff remain professionally responsible for reviewing and verifying AI-generated outputs.

Any accidental disclosure of personal information to an unauthorised AI system must be reported immediately as a potential data protection incident.

18. Photographs and Videos

EMLM may take photographs or video recordings for legitimate educational, safeguarding, administrative or operational purposes.

Where photographs or videos are intended for promotional, publicity or marketing purposes, EMLM will identify the appropriate lawful basis and obtain consent where consent is required.

Where consent is relied upon, individuals will be told how the image or recording may be used and may withdraw their consent.

Withdrawal of consent will prevent future use where consent is the lawful basis. EMLM will take reasonable steps regarding material within its control but may not always be able to retrieve material that has already been lawfully published or copied by others.

Particular care will be taken when publishing images of learners, having regard to safeguarding considerations.

19. CCTV

EMLM uses CCTV in appropriate locations for purposes including the safety and security of learners, staff, visitors and School premises.

CCTV will be operated in accordance with data protection legislation, relevant ICO guidance and EMLM's CCTV Policy.

Appropriate signage will identify areas where CCTV is operating.

Access to CCTV recordings will be restricted to authorised individuals.

Requests for CCTV footage containing an individual's personal data will be handled in accordance with applicable data protection rights.

Enquiries concerning EMLM's CCTV system should be directed to the Head of School or DPO.

20. Biometric Data

EMLM does not currently operate an automated biometric recognition system for learners.

Should EMLM consider introducing biometric technology in the future, it will undertake an appropriate legal, safeguarding and data protection assessment before implementation, including a DPIA where required.

No biometric recognition system involving learners will be introduced without compliance with the applicable legal requirements and appropriate information being provided to learners and parents/carers.

21. Data Protection by Design and Default

EMLM will consider data protection from the outset when designing or introducing systems, services, processes or technologies involving personal data.

This includes:

- Processing only the personal data that is necessary;
- Limiting access appropriately;
- Implementing appropriate technical and organisational security measures;
- Considering privacy when procuring technology;
- Maintaining appropriate records of processing;
- Reviewing retention arrangements;
- Carrying out DPIAs where required; and
- Consulting the DPO where processing may present significant privacy risks.

22. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be undertaken where processing is likely to result in a high risk to individuals' rights and freedoms. A DPIA may also be appropriate when EMLM introduces:

- Significant new technology;
- AI systems processing personal data;
- Extensive monitoring;
- New CCTV arrangements;
- processing involving significant amounts of special category data;
- automated decision-making;
- new systems involving learner profiling; or
- other processing presenting heightened privacy risks.

The DPO will advise on whether a DPIA is required.

23. Educational Technology and Third-Party Systems

Before introducing EdTech, software or other third-party systems that process personal information, EMLM will consider data protection and information-security requirements. Appropriate due diligence will include consideration of:

- What information will be processed;
- Why it is required;
- Lawful basis;
- Security;
- Supplier access;
- Retention and deletion;
- Subcontractors;
- International transfers;
- Data ownership;
- Children's privacy;
- Contractual arrangements; and
- The supplier's responsibilities following termination of the service.

Staff must not introduce software, apps or online services that process learner or staff personal data without appropriate School authorisation.

24. Data Security

EMLM will implement appropriate technical and organisational measures to protect personal information against accidental or unlawful loss, destruction, alteration, disclosure or access.

Measures will include, where appropriate:

- secure passwords and authentication;
- appropriate access controls;
- encryption;
- secure School-managed devices;
- secure email and file-sharing arrangements;
- physical security for paper records;
- secure backup arrangements;
- appropriate cyber-security measures;
- staff training;
- appropriate supplier controls; and
- procedures for reporting security incidents.

Staff must not share passwords or authentication credentials.

Personal data should only be taken off site where this is necessary and authorised, and appropriate security measures must be followed.

Staff must comply with EMLM's requirements regarding the use of personal devices, removable media, email, cloud storage and remote working.

25. Records Retention and Disposal

EMLM will not retain personal information for longer than necessary. Retention periods will be determined according to:

- legal and regulatory requirements;
- safeguarding requirements;
- educational requirements;
- contractual requirements;
- limitation periods;
- operational need; and
- relevant sector guidance.

Detailed retention periods will be set out in EMLM's Records Retention Schedule. At the end of the applicable retention period, information will be securely:

- deleted;
- destroyed;
- anonymised; or
- retained for a documented lawful reason.

Paper records containing confidential information will be securely shredded or destroyed.

Electronic records will be securely deleted in accordance with appropriate technical procedures.

Where a third party destroys records on EMLM's behalf, appropriate assurances and contractual safeguards will be required.

26. International Data Transfers

Where EMLM transfers personal data outside the UK, including where information is hosted or accessed internationally by a technology provider, it will ensure that the transfer complies with UK data protection law.

EMLM will establish that an appropriate transfer mechanism and safeguards are in place and will undertake any required assessment of the protection provided in the destination country.

The DPO should be consulted before new arrangements involving international transfers are introduced.

27. Personal Data Breaches

All suspected or actual personal data breaches must be reported immediately to the DPO or, if the DPO is unavailable, the Head of School.

Staff must not attempt to conceal a breach or delay reporting it while investigating the matter themselves.

Examples include:

- Sending personal information to the wrong recipient;
- Losing paperwork containing personal data;
- Loss or theft of a device;
- Unauthorised access to a system;
- Inappropriate disclosure of safeguarding information;
- Cyberattack or compromised account;
- Publishing identifiable information accidentally;
- Accessing information without authority; or
- Entering personal information into an unauthorised AI system.
- EMLM will investigate, contain and assess the breach promptly.

Where a breach is likely to result in a risk to individuals' rights and freedoms, EMLM will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to affected individuals, EMLM will also communicate the breach to those individuals without undue delay unless an applicable exception applies.

All personal data breaches will be documented, including breaches that are not reported to the ICO.

The procedure in Appendix 1 applies.

28. Data Protection Complaints

EMLM will maintain an accessible process for individuals to raise concerns or complaints about the way their personal information has been handled.

A complaint concerning data protection should normally be directed to the DPO. The School will:

- Acknowledge and investigate the concern appropriately;
- Consider the issues raised fairly;
- Keep an appropriate record of the complaint and outcome;
- Provide a response within the applicable statutory timeframe; and
- Provide information about the individual's right to complain to the ICO and seek an appropriate judicial remedy.

EMLM will cooperate with the ICO where required.

29. Training and Awareness

All staff will receive appropriate data protection training as part of their induction. Refresher training will be provided periodically and where:

- Legislation or guidance changes;
- New technology creates additional risks;
- School procedures change;
- Incidents indicate additional training is required; or
- Particular staff roles require additional knowledge.

Training may include:

- Recognising information rights requests;

- Secure information sharing;
- Safeguarding and data protection;
- Phishing and cyber security;
- Personal data breaches;
- Use of AI;
- Handling SEND and health information; and
- Secure use of School systems.

Relevant governors and leaders will also receive appropriate data protection awareness or training.

30. Monitoring and Review

The DPO will monitor EMLM's data protection arrangements and advise the School on changes required. The policy will be reviewed at least annually and sooner where there is:

- A significant change in legislation;
- New ICO or DfE guidance;
- A significant change in EMLM's processing activities;
- Introduction of significant new technology;
- A serious data protection incident; or
- Evidence that existing arrangements require improvement.

The policy will be approved by the Proprietor in accordance with EMLM's governance arrangements.

Appendix 1 – Personal Data Breach Procedure

1. Immediate Reporting

Any member of staff who becomes aware of an actual or suspected personal data breach must report it immediately to the DPO.

If the DPO is unavailable and the matter is urgent, it must be reported to the Head of School.

Staff should provide as much information as possible but must not delay reporting because all the facts are not yet known.

2. Immediate Containment

Where possible and safe to do so, immediate steps should be taken to contain the breach. These may include:

- Recalling an incorrectly addressed email;
- Contacting an unintended recipient;
- Disabling or securing a compromised account;
- Changing passwords;
- Recovering documents or devices;
- Removing information published accidentally;
- Restricting access to affected systems; or
- Contacting EMLM's IT provider.

Evidence relevant to the incident must be preserved.

3. Investigation

The DPO will coordinate an appropriate investigation. The investigation will establish, where possible:

- What happened;
- When it happened;
- When EMLM became aware of it;
- What personal information is affected;
- Whose information is affected;
- The approximate number of people and records involved;
- Whether special category, criminal offence or safeguarding information is involved;
- Who has or may have accessed the information;
- Likely consequences;
- Whether information can be recovered or contained; and
- What further action is necessary.

Staff are expected to cooperate fully with the investigation.

4. Risk Assessment

The DPO will assess the likely risk to affected individuals. Factors may include:

- sensitivity of the information;
- volume of information;
- vulnerability of affected individuals;
- whether children are affected;
- whether safeguarding information is involved;
- whether information was encrypted;
- who received or accessed the information;
- likelihood of misuse;
- potential physical, emotional, financial or reputational harm; and
- effectiveness of containment measures.

5. ICO Notification

Where the breach is likely to result in a risk to individuals' rights and freedoms, the DPO will ensure that the ICO is notified without undue delay and, where feasible, within 72 hours of EMLM becoming aware of the breach.

Where all information is not available within 72 hours, an initial report may be made and additional information supplied subsequently as appropriate.

The decision whether or not to notify the ICO will be documented.

6. Notification of Affected Individuals

Where a breach is likely to result in a high risk to an individual's rights and freedoms, EMLM will notify affected individuals without undue delay unless an applicable legal exception applies. Communications will use clear and accessible language and explain:

- What happened;
- The likely consequences;
- Steps EMLM has taken or proposes to take;
- Practical steps the individual can take to protect themselves; and
- How to contact EMLM or the DPO.

Communication with learners will take account of their age, understanding, SEND and communication needs.

7. Safeguarding Information

Where a breach involves safeguarding or child protection information, the DPO will immediately involve the Designated Safeguarding Lead. The DSL and DPO will consider whether information needs to be shared with:

- Relevant safeguarding partners;
- The local authority;
- Children's social care;
- Police; or
- Other relevant agencies.

Safeguarding action must not be delayed while the data protection assessment is completed.

8. Emails Sent to the Wrong Recipient

Where confidential information is sent to an unintended recipient:

- The sender must immediately notify the DPO;
- An attempt should be made to recall the message where technically possible;
- The recipient should normally be contacted promptly and asked to permanently delete the message and attachments and not copy, use or disclose the information;
- Confirmation of deletion should be sought where appropriate;
- IT support should be involved where necessary; and
- The DPO will assess the risk and determine whether further notification or action is required.

9. AI-Related Breaches

Where personal, confidential, safeguarding or special category information is accidentally entered into an unauthorised AI system, this must be reported immediately. The DPO will consider:

- What information was entered;
- whether individuals can be identified;
- whether the provider retains prompts or outputs;
- whether information may be used for model training;
- where the information is processed;
- whether deletion can be requested;
- whether third parties may have access; and
- whether notification to affected individuals or the ICO is required.

10. Recording and Learning from Breaches

EMLM will maintain a record of personal data breaches regardless of whether they are reported to the ICO. Records will include:

- the circumstances and cause;
- information affected;
- risk assessment;
- containment measures;
- notifications made;
- decisions and reasons;
- remedial action; and
- lessons learned.

Following a significant breach, the DPO and relevant leaders will review whether changes are required to:

- procedures;
- systems;
- access controls;
- contracts;
- risk assessments;
- DPIAs;
- staff training; or
- School policies.

Recurring incidents and trends will be reported to senior leadership and the Proprietor or Independent Executive Board as appropriate.