Melrose Education
SCHOOL

GDPR Policy

Reviewed by:	Andrew Patterson, Compliance Manager
Date:	1 August 2023
Last reviewed on:	01 September 2022
Next review due by:	31 July 2024
Version control:	1
Approved by:	Tracey Storey, CEO

Contents

Melrose Education will maintain certain personal data about individuals for the purposes of satisfying operational and legal obligations whilst fully complying with the current legislation. We recognise the importance of the correct, lawful, and ethical treatment of personal data and will ensure all employees fully understand this policy both at the time of signing and giving express consent and their rights to withdrawal of said consent. We will respect the privacy rights of all individuals, including employees, contractors, customers, potential customers, and business contacts regarding the processing of their personal information.

The type of personal data the Company may require includes information about current, past, and prospective employees, parents, learners, local authorities, suppliers, and others with whom it communicates. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the General Data Protection Regulation legislation which came into force in May 2018.

The Company fully endorses and adheres to the seven principles laid out in Article 5 of the UK GDPR, and these principles form the foundation to our approach to processing personal data. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation, and storage of personal data. Employees and any others who obtain, handle, process, transport, and store personal data for the Company must adhere to these principles.

7 GDPR Principles
The principles are:

1. Lawfulness, fairness, and transparency – i.e., you must have a lawful reason for collecting personal data and must do it in a fair and transparent way.
2. Purpose limitation – i.e., data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those.
3. Data minimisation – i.e., you must not collect any more data than is necessary. Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy – i.e., data must be accurate and there must be mechanisms in place to keep it up to date. Data must be erased or rectified without delay where applicable.
5. Storage limitation – i.e., data must not be kept for any longer than needed.
6. Integrity and confidentiality (security) – i.e., personal data must be processed in a way that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
7. Accountability – The Data Controller is responsible for and will ensure written procedures and management documents are in place to demonstrate compliance with Article 5(1) (the 6 preceding Principles).

Satisfaction of Principles
To meet the requirements of the principles, the Company will:

- Observe fully the conditions regarding the fair collection and use of personal data.
- Meet its obligations to specify the purposes for which personal data is used.
- Collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirement.
- Ensure the quality of personal data used.
- Regularly review the amount of data collected and minimise this where possible or appropriate.
- Apply strict checks to determine the length of time personal data is held.
- Ensure that the rights of individuals about whom the personal data is held can be fully exercised.
- Take the appropriate technical and organisational security measures to safeguard personal data.
- Ensure that personal data is not transferred abroad without suitable safeguards.
- Ensure appropriate written procedures are in place, for example our internal privacy policy, and including documented decision-making processes to ensure traceability.
- Provide appropriate and regular training to relevant staff on the principles of the GDPR and our own internal procedures, including sending as and when appropriate updates to any relevant policies and procedures, including improvement plans.
- Notify the ICO (Information Commissioner's Office) of a data breach within 72 hours of becoming aware of the breach.
- Adhere to and regularly review our Privacy Management Programme.
- Appoint a Company DPO who has overall responsibility for all policies and procedures.
- Ensure each school has an appointed Designated Data Lead to be responsible for the implementation of the Privacy Management Programme.
- Ensure robust Cyber Security policies and procedures are in place.
- Regularly review all data protection and cyber security policies and procedures and identify areas for improvement (where applicable) at each review.

Status of the Policy

This policy has been approved by the Directors and any breach will be taken very seriously. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their school's designated DDL in the first instance.

Individual Rights

All individuals who are the subject of personal data held by the Company are entitled to:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

This may include but not be limited to:

- asking what information is held about them and the reasons why it is being held.

- asking how to gain access to data held about them.
- being informed about how the data is kept up to date.
- being informed about what the Company is doing to comply with its obligations.

Employee Responsibilities

All employees are responsible for:

- checking that any personal data that they provide is accurate and up to date.
- informing the Company of any changes to information which they have provided, e.g., change of address.
- checking the accuracy of any information that the Company may send out from time to time, giving details of information that is being kept and processed.
- giving or withdrawing their express consent for the Company to use personal data.

Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted.

All staff are responsible for ensuring that:

- any personal data which they hold is kept securely.
- personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Rights to Access Information

Employees and other subjects of personal data held by the Company have the right to make a subject access request about information that is being kept about them on computers/computer systems/databases and paper-based data held in manual filing systems. Any person who wishes to exercise this right should make the request in writing to their principal. The Company will ensure any requests for information are provided free-of-charge.

Employees have the right to "be forgotten" in that once it is no longer necessary for the Company to hold information, the employee can request that it be deleted. The Company will be responsible for removing any external links to any information held.

The Company aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within one month unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request. Any information provided will be done so in an accessible, concise, and intelligible format, and will be disclosed securely. Information requested in this way will only be refused if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

Subject Consent

The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race, or gender then express consent to process the data will be obtained. Processing may be necessary to operate the Company's policies, such as health and safety and equality and diversity.

Retention of Data
The Company will keep some forms of information for longer than others. All staff are responsible for ensuring that both legal and statutory retention requirements are adhered to, and that information is not kept for longer than necessary (in accordance with the GDPR Retention Schedule and the retention period information below).

Confidentiality – Data Protection
You should be aware that the obligations placed on you because of the law and this policy are in addition to the duty of confidentiality which you owe to the Company in respect of all information (including personal data) processed by you; by the Company; its customers; employees; suppliers and any other data subjects.

You must keep all personal data which you process on behalf of the Company completely secret and confidential and must not disclose any such information unless authorised to do so.

Termination
You should be aware that all information (including personal data) processed by employees during their employment with the Company (whether in a manual or automated fashion) is, and will, remain the property of the Company. On termination of your employment with the Company, you must promptly return the original and any copies (whether in manual or automated form) of any information including personal data obtained by you during your employment to the Company.

GDPR and Safeguarding

Working Together to Safeguard Children 2018 (1:27) states:

"The Data Protection Act 2018 and General Data Protection Regulations (GDPR) do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children."

Retention Periods – Employment

Record Type	Retention Period
Absence records, including return to work forms (maternity (including MAT B1s), paternity, sick, special, unpaid leave)	Duration of absence period + 3 years
Annual leave records, including extended holiday records	Relevant holiday year + 2 years
Application forms, CVs, and interview notes (unsuccessful candidates)	Conclusion of recruitment process + 6 months
Career breaks	Duration of employment
Counselling records	Date of meeting + 1 year
DBS disclosure information	Date of recruitment decision + 6 months
Disciplinary, grievance and dismissal records	Date of decision + 5 years
Exit interviews	End of employment + 1 year
Flexible working records	Date of decision + 1 year
Health Records (within Occupational Health)	Date of referral + 10 years
National Minimum Wage records	End of pay reference period following the one the records cover + 3 years
Parental leave	Date of leave + 5 years
Personal details – subject to change – 'old' details (e.g., address, contact details, trade union membership, bank details, next of kin)	Date of change + 6 months
Redundancy details, including calculations of payments, refunds, notification to the Secretary of State	Date of redundancy + 7 years
References given by the Company	End of employment + 1 year
Resignation letters	Date of resignation letter + 7 years
Subject access requests	Date of request + 3 years
Working time records (including exceptions)	Date on which record was made + 2 years

Application forms, CVs, interview notes and references (successful candidates)	Duration of employment + 7 years
Contract, contractual schedule, offer letter, start date letter, health questionnaire, right to work records (including passport or Visa details), qualifications, contract variations, changes to	Duration of employment + 7 years
Job data (location, department, job code, position).	Duration of employment + 7 years

Record Type	Retention Period
Supervision, performance, appraisal, assessment, and training records	Duration of employment + 7 years
Personal details - core (e.g., name, date of birth, gender, race or ethnic origin, health information, national insurance)	Duration of employment + 7 years
Condensed listing reports (payments and deductions)	Date of change + 10 years
Earnings records (including bonuses, expenses, maternity pay, overtime, payments in kind, salary, sick pay, and wages)	Duration of employment + 7 years (or to end of any tax enquiry, if longer)
Income tax and NI returns, income tax records and correspondence with HMRC	End of financial year to which they relate + 7 years
Pension payment records	Duration of entitlement to benefit + 7 years

Retention Periods – Schools

Record Type	Retention Period
Staff signing in and out registers, learner's registers	21 years
Outings documentation including risk assessments	7 years
Health and safety documentation including fire records	7 years
Complaints documentation	7 years
Accidents and Incidents relating to a specific learner	21 years
EHC Plans and other learner case notes	21 years
Safeguarding and child protection case notes	21 years

Retention Periods - Office

Record Type	Retention Period
HR records – see Employment section above	7 years
Insurance documentation	7 years
Finance documentation	7 years
Health and safety documentation	7 years
Property documentation	7 years