MI Skills Development Centre

General Data Protection and Retention Regulation Policy

DPA Reform UK GDPR

2025 - 2028

MI ComputSolutions Training

GENERAL DATA PROTECTION REGULATION POLICY

DATA PROTECTION ACT 1998, reformed May 25th 2018, with UK General Data Protection Regulation (UK GDPR).

The UK GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). Compliance with UK GDPR required a change in many policies and procedures and it needs all staff, volunteers, service users, members, supporters and donors to embrace new procedures.

The above regulation was introduced to regulate how personal data held either on computer or within a manual filing system. This includes regular review of our privacy notice. Our privacy notices set out what we collect, what we do with it, how long we keep it for and your rights under the UK General Data Protection Regulation (UK GDPR).

When there is an important change, we will remind you to take a look and this is so you are aware of how we use your data and what your options are.

As an organisation it is our responsibility to ensure that the documentation held is relevant, accurate and where necessary, kept up to date. Any data held shall be processed fairly and lawfully and in accordance with the rights of data subjects under the Act 2018.

As a learner, volunteer and employee under UK GPDR it allows you as an individual to exercise your rights regarding your personal data by assisting you in correctly identifying the personal data we are processing on your behalf.

Personal data is defined in the UK GDPR as:

"'personal data' means any information relating to an identified or identifiable natural person ('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".

This means personal data has to be information that relates to an individual. That individual must be identified either directly or indirectly from one or more identifiers or from factors specific to the individual.

MI ComputSolutions processes personal data in the 2 following ways:

- personal data processed wholly or partly by automated means (that is, information in electronic form); and

- personal data processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is, manual information in a filing system).

MI ComputSolutions processes personal data for core business purposes only. These are

- Staff Administration
    - This is processing for the purposes of appointments, removal, pay, discipline, superannuation, work management and other personal matters concerning you as a staff.
- Accounting and Record Keeping
    - This is a process for the purposes of keeping accounts relating to our business or other activities we carry out; staff salaries, keeping records of purchases, deliveries or services take place and making financial accounts to help us to carry out our business

MI ComputSolutions is also a processor of personal data acting on behalf of various controllers. As part of our commitment to transparency we have updated the Privacy Notice for our learners which clearly communicates to individuals the lawful basis for processing personal data, summarising the information held on record about learners, why it's held and the third parties the data is shared with. As an organisation we have different organisations that uses the personal data we process for different purposes Copy of privacy notice for learners - https://www.gov.uk/government/publications/lrs-privacy-notices

Due to the sensitivity of the data processed, we maintain a higher level of protection, and this is referred to as special categories of data. Personal data is

- kept secure only for the purposes for which the personal data is processed. The personal data may be stored for longer periods and will be stored no longer than the retention period for archiving purposes in the public and statistical purposes with storage limitations.
- protect it from inappropriate disclosure;
- be open about how we are collecting the information; and
- ensure we are justified in any processing.

As a learner, volunteer and employee you will have the right, upon written request, to be told what personal data about you is being processed. You will also have the right to be informed of the source of the data and to whom it may be disclosed and its purpose.

We are not obliged to supply this information unless you make a written request and for such requests, a fee of £10 may be payable.

1. The Data Protection Act reformed 2018 regulates the way in which personal data about you is processed and used. Although the Act does apply to all records about learners, volunteers and employees held we consider that many of the principles in the new Act represent best practice and we have therefore decided to issue this policy to all learners, volunteers and employees. We do not intend to alter the way in which we currently keep or use information about you and the purposes for which we keep them and its retention period.

2. Throughout your learning, volunteering and employment and for as long a period as is necessary following the termination of your volunteering/employment or completion and achievement of your programme the company will need to keep certain information about you for purposes connected with your learning, employment/volunteering and

3. The records kept and obtained during your volunteering/recruitment include tax code, N.I. etc., and information about your performance, details of your grade and job duties; health records; absence records including holiday records and self-certification forms; details of any disciplinary investigations and proceedings; training records; contact names and addresses; correspondence with us and other information that you have given us.

4. We believe these uses are consistent with our employment relationship and with the principles of the Data Protection Act reformed 2018 (UK GDPR). The information we hold will be for management and administrative use only but we may, from time to time, need to disclose some information we hold about you to relevant parties (e.g. where we are legally obliged to do so by the Inland Revenue or where requested to do so by you for the purposes of giving a reference)

Privacy notice

What information is collected and why?

As part of the funding arrangements for this programme we must collect evidence of your eligibility and information about your participation in the programme. This will include ID checks, employment status and other evidence required for the programme you are enrolling on. We also need to keep information on your progress through the programme.
This programme is funded by the, the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council. We will only ask you for information required by the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council.

To enrol on a project funded under the Greater London Authority (GLA), the Department for Education, Lambeth Council, and Wandsworth Council you must agree to provide the requested information because the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council are not able to access the funding for the project without collecting the

required information. The Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council are registered to process personal data under the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (UK GDPR) and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

The purposes of the data processing

The information you provide to the provider that runs the project and the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council will be used to evaluate this project and to report to the provider that runs the project, the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council for monitoring purposes.

Your information will also be shared with research organisations working on behalf of the Greater London Authority (GLA), the Department for Education (DfE). Lambeth Council, and Wandsworth Council who may contact you to discuss your involvement in the project for research purposes. Participation in research is voluntary, and you will be asked to consent before taking part in any research activity you may be contacted about.
The Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council may also link your personal details to official administrative records in order to monitor your employment status before your support began and 6 to 12 months after you left. This information may also be shared with research organisations working on behalf of the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council however individuals will not be identifiable, and you will not be contacted about this research.

Data will not be used or shared for any commercial or marketing purposes.
At all times your information will be kept securely, and nobody will have access to it that shouldn't.

The lawful basis for the processing

For the purposes of UK GDPR, the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council are the data controllers in respect to information processed which relates to all participation in the Programmes. The Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council grant beneficiary organisations are data processors in respect to information processed which relates to participants in the operations and projects funded by the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council.

The retention periods for the personal data

All personal data held by the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council or research contractors for the purposes of evaluation will be permanently deleted no more than six months after the research has been completed (i.e. when the final report is published on GOV.UK).
Personal data held by the Greater London Authority (GLA), the Department for Education (DfE), Lambeth Council, and Wandsworth Council for all other purposes as required will be retained in line with the current guidance on GOV.UK at:

https://www.gov.uk/government/publications/record-keeping-and-retention-guidance-for-fe-training-providers/record-keeping-and-retention-information-for-training-providers

The rights available to individuals in respect of the processing

Information Produced on behalf of: AQA, City & Guilds, CCEA, NCFE, OCR, Pearson and WJEC

Information for candidates – Privacy Notice

General and Vocational qualifications

The JCQ awarding bodies will process your personal data in accordance with the Data Protection Act reformed 2018, and UK General Data Protection Regulation, and any regulatory requirements as specified by the qualification regulators of England, Wales, Northern Ireland and Scotland.

Correspondence on any aspect of a candidate's examination or assessment will only be conducted between the awarding body and the head of the centre, a member of the senior leadership team or the examinations officer.

Awarding bodies will undertake the following administrative activities in relation to the processing and exchange of candidates' personal data:

1. Personal data relating to the name(s), date of birth, gender, Unique Candidate Identifier (UCI) or Unique Learner Number (ULN) of an individual candidate will always be collected by an awarding body for the purposes of examining and awarding qualifications. In some cases, additional information, which may include sensitive personal data relating to health, will also be collected to support requests for access arrangements and reasonable adjustments and/or special consideration. Such personal data will be supplemented by the results of examinations and assessments undertaken by the respective candidate.
2. A candidate's personal data will only be collected from registered examination centres in the context of examination entries and/or certification claims.
3. Such data collected will not be used by an awarding body other than for examination administration purposes, conducting examinations and assessments and the issuing of examination results and certificates. Candidates' personal data including examination results and outcomes of any reviews of marking, reviews of moderation and appeals may be shared by the awarding body with the centre which entered the candidates, as well as within a consortium or Academy Trust of which the centre is a member.
4. Personal data within candidates' work will be collected and processed by an awarding body for the purposes of marking, issuing of examination results and providing candidates with access to post-results services. Examination results will be retained for a minimum of forty years. In order for an awarding body to achieve this, some personal information may be transferred to third parties such as examiners, who may in some instances, reside outside the European Economic Area.
5. Awarding bodies may be required to provide a candidate's personal data to educational agencies such as DfE, WG, DE, the GLA, regulators, HESA, UCAS, Local Authorities, and Learning Records Service (LRS). Additionally, candidates' personal data may be provided to a central record of

qualifications approved by the awarding bodies for statistical and policy development purposes.

6. Some of the information candidates supply will be used by the DfE to fulfil its statutory functions, issue/verify a candidate's Unique Learner Number (ULN) and update/check a candidate's Personal Learning Record.
7. The DfE may share a candidate's ULN and Personal Learning Record with other education related organisations, such as a careers service, a candidate's school or college, Government Departments and public bodies responsible for education. Further details of how information is processed and shared can be found at: http://www.learningrecordsservice.org.uk/
8. Awarding bodies are obliged to confirm what personal data is held, what it is held for, to whom the data is to/may be disclosed to, and disclose the information that they hold about data subjects, (e.g. the candidates) within 40 days of receiving a formal request for disclosure, subject to the application of any relevant exemptions under the Data Protection Act reformed 2018. Candidates should make an application to the appropriate awarding body's data protection officer. Awarding bodies may charge a fee for this service.
9. If you have not reached the age of 16, you may first wish to discuss this Privacy Notice with your parent or carer. Awarding bodies, schools, Department for Education (DfE), Welsh Government (WG), Department of Education Northern Ireland (DE), Local Authorities, regulators, Ofsted, and the GLA are all 'data controllers' under the Data Protection Act reformed 2018. They will determine the purpose(s) for which 'personal data' (information about living individuals from which they can be identified) is processed and the way in which that processing is undertaken.

It is a requirement for data controllers to provide data subjects (individuals who are the subject of personal data) with details of who they are, the purposes for which they process the personal data, and any other information that is necessary to make the processing of the personal data secure and accurate, including any third parties to whom it may be passed to.

Procedure for Retention of Records

Data Retention Policy

1. MI ComputSolutions processes personal data in accordance with the principles of the Data Protection Act reformed 2018 UK GDPR,

2. Only personal data relating to the names, date of birth, gender and unique candidate identification number of individual candidates will be collected. To these will be added the results of all examinations and assessments undertaken by the candidates.

3. Personal data will not be used by MI ComputSolutions for any purposes other than the legitimate administration of examination, assessments, training and certification.

4. Personal data will be provided to government departments and agencies, including DfE and GLA for the compilation of statistics relating to examination results and performance indicators.

5. Personal data may be consolidating with that from other participating awarding bodies to provide a central record of candidate achievement.

6. The personal data identified in paragraph 11 will be kept for as long as is necessary in the archive of candidate achievement for as required by the funding body and awarding organisations.

7. All records are to be retained for three years from the date the candidate achieved the qualification.

8. All records for DfE/GLA are to be retained for 6 years from Financial Year End after last payment made for learners that did access this funding provision from the date that Managing authority has made the final payment relating to that claim.

Data Retention Schedules

File	Retention Period
Learner Work and Assessment • Candidate Cumulative Assessment record • Portfolio of Evidence • Certificates & Receipt of Certificates • Candidate assessment records detailing who assessed what and when, the assessment decision, the	2 years from end of course.

assessment methods used for each unit/component and the location of the supporting evidence. • Records of internal verification activity detailing who verified what and when, details of the sample selected and its rationale, records of internal verifier standardisation meetings. • Records of assessor support meetings, assessor • Verifier competence records and monitoring records of assessor/internal verifier progress towards achievement of the relevant assessor and internal verifier qualifications. • Assessment team meetings and standardisation meetings. External verifier visit reports • Records of Staff Development Plans • Records of Appeals and Complaints	
Learner file (funded through DfE, LC, GLA, HO, DWP) (see below Guidance for reference) • Data Capture Form • ILR • ILP • Learning Agreement • Reviews • Attendance Records • Progress Review • Job Outcome Evidence • Initial Assessment • Certificates • Additional Learning Support Evidence • Addition Social Needs Evidence • Exit Review	6 years from Financial Year End after last payment made by the Managing Authority and confirmation will be sought from the Managing Authority before destroying any documents.

Accountability Framework for Joint Controller and Processor

MI ComputSolutions will ensure all staff at induction and as part of CPD completes the self-assessment tool kit **-** https://ico.org.uk/for-organisations/advice-for-small-organisations/getting-started-with-gdpr/data-protection-self-assessment-medium-businesses/

As part of our development, we do adhere to the ICO Accountability Framework which makes us responsible for complying with the legislation and ability to demonstrate compliance. It is used as part of our staff induction and staff CPD process for all those responsible for personal data processing including senior leaders to assess understanding and compliance with data protection law and what needs to be done in keeping people's personal data secured.

Staff complete a GDPR training course at the start of their employment, such as https://measuredcollective.com/courses-list/free-gdpr-training-course/. The Data Protection Officer (DPO) carries out update training for all staff when any changes to GDPR legislation come into force. This process enhances good information handling of personal data, whilst

making sure personal information is accurate, relevant and safe, and that all staff are aware of current legislation.

Learner Certification

MI ComputSolutions will ensure that:

- All certificates are issued to all candidates without delay and regardless of any disputes (such as non- payment of fees).
- A signed record is kept of the certificates that are issued
- All unclaimed certificates are retained under secure conditions for a minimum of 12 months from the date of issue
- All unclaimed certificates are returned to the awarding body if not sent to the learner

Storage and Archiving

MI ComputSolutions will ensure that:

- A member of staff is nominated who has the responsibility for storage and archiving.
- An area is made available that provides secure lockable storage with limited access
- All venues used for examinations and assessments, records, and secure storage facilities are open to inspection.
- All assessments, coursework and portfolios are stored safely and securely until the deadline for an enquiry about results has passed or until any enquiry (results, appeal or malpractice enquiry) has been completed, whichever is later. This includes materials stored electronically
- All portfolios are stored safely and securely until the deadline 2 years from end of course for an enquiry about results has passed or until any enquiry (results, appeal or malpractice enquiry) has been completed, whichever is later. This includes materials stored electronically
- All stored portfolios kept after the 2 years from end of course not collected will be destroyed safely and securely
- Confidentiality of work and data is respected by not allowing them to be read or photocopied by any person prior to marking, without permission of awarding body
- Personal data and assessment, coursework and portfolios are held available to candidates when requested
- All documents will be securely stored and archived internally for the period stated on the retention schedule

	Future Review Dates					
	2020	2021	2023	2024	2025	2028
Date reviewed	Oct	March	Aug	Aug	June	

Personal Data Breach Management Procedure

1. Procedure Statement

MI ComputSolutions is committed to ensuring the security and confidentiality of personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We recognise the importance of promptly managing and investigating personal data breaches to minimise potential harm and meet our legal obligations. This policy sets out the process for identifying, reporting, managing, and mitigating personal data breaches.

2. Scope

This policy applies to all employees, contractors, and third parties handling personal data on behalf of MI ComputSolutions. It covers all suspected or confirmed breaches involving personal data, whether held electronically or in physical form.

3. Definition of a Personal Data Breach

A personal data breach is defined as a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include:

- Sending personal data to the wrong recipient.
- Loss or theft of devices containing personal data.
- Unauthorised access to personal data by an internal or external party.
- Cyberattacks, such as phishing or ransomware incidents.
- Accidental deletion or modification of personal data without backup.

4. Personal Data Breach Management Procedure

Step 1: Identification & Reporting

- Any staff member who becomes aware of a potential personal data breach must report it immediately to the **Data Protection Officer (DPO) or designated responsible person**.
- Reports should be made using the **Personal Data Breach Report Form (Appendix A)**, including details of what happened, when, and how the breach was discovered.

Step 2: Containment & Risk Assessment

- The DPO or responsible team will take immediate action to contain the breach and prevent further loss or unauthorized access.
- An initial risk assessment will be conducted to determine:
    - The type and volume of personal data involved.
    - The potential impact on individuals.
    - Whether the breach is likely to result in a risk to data subjects' rights and freedoms.

Step 3: Notification & Communication

- If the breach is likely to result in a high risk to individuals, the affected individuals must be notified without undue delay.
- If the breach is **reportable**, the Information Commissioner's Office (ICO) must be notified **within 72 hours** of becoming aware of the breach, detailing:
    - The nature of the breach.
    - The categories and approximate number of individuals affected.
    - Possible consequences and remedial actions taken.
    - Contact details for further information.
- Where required, the organisation will notify other relevant regulatory bodies, funders or stakeholders.

Step 4: Investigation & Remediation

- A full investigation will be conducted to establish the root cause of the breach and identify necessary corrective actions.
- Actions may include:
    - Improving security controls.
    - Revising policies and procedures.
    - Providing additional staff training on data protection.
    - Enhancing IT security measures.

Step 5: Record-Keeping & Review

- All breaches, whether reportable or not, must be recorded in the **Data Breach Register (Appendix B**)
- A post-incident review will be conducted to assess lessons learnt and improve future data protection measures.
- The policy and procedures will be reviewed periodically to ensure continued compliance with UK GDPR.

5. Roles & Responsibilities

- **All Employees & Contractors:** Responsible for reporting any suspected breaches immediately.
- **Data Protection Officer (DPO):** Oversees breach management, ensures compliance, and reports to senior leaders, board and the ICO if necessary.
- **IT & Security Team:** Assists in containing breaches and implementing security enhancements.
- **Senior Management:** Provides oversight and ensures that necessary resources are allocated for data protection.

6. Compliance & Consequences of Non-Compliance
Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Serious breaches may also lead to legal consequences, including regulatory fines from the ICO.

7. Contact Information
For any data breach concerns or further information, please contact:

Data Protection Officer
Paul McDermott – Paul.M@micomputsolutions.co.uk
Bola Sobowale – Bola.s@micomputsolutions.co.uk

This reporting procedure ensures that MI ComputSolutions meets its obligations under UK GDPR and takes appropriate action to protect personal data and mitigate risks associated with data breaches.

Appendix A: UK GDPR Data Breach Reporting Form

Date and Time of Notification of breach	
Notification of breach and to whom Name Contact Details	
Details of breach	
Nature and Content of Data Involved	
Number of Individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner **informed Time and method of contact** https://ico.org.uk/for-organisations/report-a-breach/	
Funders Informed if relevant Time and method of contact Name of person contacted	

Contact details	
Stakeholders Informed if relevant Time and method of contact Name of person contacted Contact details	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact?	
Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed Board Briefed	
Assessment of ongoing risk	

Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	

Appendix B: Security Incident Record Form

DATA SECURITY INCIDENT LOG This log is to be used to record / note data security breaches			
Date of Incident	**Risk Identification and Classification** Include the steps and evidence used to identify and classify the risk.	**Incident Review Details: Meeting** Record the actions taken to report the breach; the meeting date and actions taken as a result of the breach	**Name and Signature** Officer investigating breach