MORLEY COLLEGE LONDON

Data Protection Policy

POLICY OWNER:	Chief Planning and Data Officer / Data Protection Officer
FINAL APPROVAL BY:	Governing Body
Policy Category:	Corporate
Approved by Policy Committee:	9 June 2023
Approved by Governing Body:	17 July 2023
Review Date:	July 2027

1. Introduction, Purpose and Scope of Policy:

1.1 Morley College London is committed to protecting the privacy and confidentiality of personal data collected and processed as part of its activities.

1.2 This Data Protection Policy outlines the principles and procedures we follow to ensure compliance with the applicable data protection laws in the United Kingdom, including the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK GDPR) which sits alongside it.

1.3 The purpose of this policy is to ensure the college's compliance with data protection laws, protect the privacy and confidentiality of personal data, and establish a framework for responsible and secure data handling practices. The policy aims to promote transparency, fairness, and accountability in the processing of personal data by providing guidelines and procedures to be followed by all individuals involved in handling personal data within the college.

1.4 This policy applies to all personal data collected, processed, and stored by Morley College London, regardless of its format (electronic or manual). The policy covers personal data relating to students, staff, contractors, visitors, and any other individuals whose data is collected and processed by the college. It encompasses all areas and departments within the college, including administration, curriculum, people operations, and any other activities that involve the handling of personal data.

1.5 The policy applies to all individuals, including employees, contractors, volunteers, governors and any other individuals who have access to personal data in the course of their duties or engagements with the college. It sets out the responsibilities and obligations of these individuals in relation to the protection of personal data and compliance with data protection laws.

2. Equality and Diversity Analysis Screening:

2.1 In accordance with the College's Equality and Diversity Policy, the development of this policy complies with the Equality Act 2010 in ensuring due regard to eliminating discrimination, advancing equality of opportunity and fostering good relations.

2.2 An equality analysis will be completed if there is a risk the policy may affect different groups protected from discrimination. Consultation will be carried out with staff. If an equality analysis is required, the Chairs of the Equality, Diversity and Inclusion Steering Group will advise on completion and the analysis is to be included as an appendix to the policy.

3. Applicability:

3.1 The policy is intended to establish a framework for data protection practices within the college, ensuring that personal data is handled lawfully, fairly, and transparently. It outlines the responsibilities of the college as a data controller, the role of the Data Protection Officer (DPO), and the obligations of data processors engaged by the college.

4. Definitions:

4.1 Personal Data: Any information that relates to an identified or identifiable individual. This includes but is not limited to names, contact details, identification numbers, financial information, academic records, and any other data that can be used to directly or indirectly identify an individual.

4.2 Special categories of personal data, as defined by the UK GDPR, refer to sensitive information that requires heightened protection due to its sensitive nature. These categories include:

4.2.1 Racial or Ethnic Origin: Personal data that reveals an individual's racial or ethnic background, including information related to race, ethnic origin, nationality, or colour.

4.2.2 Health and Medical Data: Personal data concerning an individual's physical or mental health, medical conditions, disabilities, medical treatments, or genetic information.

4.2.3 Religious or Philosophical Beliefs: Personal data indicating an individual's religious or philosophical beliefs, including religious affiliations, practices, or memberships.

4.2.4 Political Opinions: Personal data relating to an individual's political opinions or political party affiliations.

4.2.5 Trade Union Membership: Personal data indicating an individual's membership in a trade union or professional association.

4.2.6 Sexual Orientation and Gender Identity: Personal data revealing an individual's sexual orientation or gender identity.

4.2.7 Biometric Data: Personal data obtained from unique biological characteristics, such as fingerprints, facial recognition, or DNA profiles, which are used for identification purposes.

4.2.8 Genetic Data: Personal data derived from the genetic characteristics of an individual, such as DNA analysis or genetic testing results.

4.3 *Data Subject:* The individual to whom the personal data relates, who can be identified directly or indirectly through the information collected.

4.4 *Data Controller*: The entity or organisation that determines the purposes and means of processing personal data. In this case, Morley College London acts as the data controller for the personal data it collects and processes.

4.5 *Data Processor*: A third party or organisation that processes personal data on behalf of the data controller. This may include service providers, vendors, or contractors that handle personal data on behalf of Morley College London.

4.6 *Processing*: Any operation or set of operations performed on personal data, such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.

4.7 *Consent*: The freely given, specific, informed, and unambiguous indication of a data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

4.8 *Privacy Notice*: A statement or document provided to data subjects that informs them about the processing of their personal data. It outlines the purposes, legal basis, retention periods, and rights of individuals in relation to their personal data.

4.9 *Data Protection Officer (DPO)*: A designated person within Morley College London responsible for overseeing data protection compliance, providing guidance, and acting as a point of contact for data subjects and supervisory authorities.

4.10 *Data Breach*: A security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. A data breach may pose risks to the rights and freedoms of individuals.

4.11 *Information Commissioner's Office (ICO)*: The independent authority in the United Kingdom responsible for promoting and enforcing data protection laws. The ICO oversees compliance, provides guidance, and has the power to investigate and impose penalties for violations of data protection regulations.

5. Statutory and regulatory requirements:

5.1 The UK GDPR is a comprehensive data protection regulation that sets out the legal framework for the protection of personal data across the European Union (EU), including the United Kingdom. It establishes various rights and obligations related to the processing of personal data.

5.2 The Data Protection Act 2018 is the primary legislation in the UK that supplements the UK GDPR. It provides additional provisions and exemptions specific to the UK context, including provisions related to law enforcement processing, intelligence services, and research.

5.3 The Information Commissioner's Office (ICO) is the UK's independent authority responsible for enforcing data protection laws and promoting good data protection practices. The ICO provides guidance, advice, and enforcement actions related to data protection.

5.4 Privacy and Electronic Communications Regulations (PECR) complement the UK GDPR and govern electronic communications and marketing activities. It sets out rules related to electronic marketing, the use of cookies and similar technologies, and the security of electronic communications.

5.5 The Human Rights Act (1998) incorporates the European Convention on Human Rights (ECHR) into UK law. It includes the right to respect for private and family life, which is closely related to the protection of personal data.

5.6 Specific requirements apply to the processing of employee data, such as employment contracts, payroll processing, and employee monitoring. These include obligations under employment laws, such as the Equality Act 2010, and relevant regulations related to employee privacy and data protection.

6. Policy Objectives:

6.1 The primary objective of the policy is to ensure compliance with applicable data protection laws in the United Kingdom, including the UK GDPR and the Data Protection Act 2018. The college aims to adhere to the legal requirements and obligations related to the processing of personal data.

6.2 The policy aims to uphold the data protection principles of the UK GDPR.

6.3 The policy recognises and respects the rights of individuals regarding their personal data.

6.4 The policy highlights the importance of regularly reviewing and updating the data protection practices to ensure ongoing compliance with data protection laws. The college aims to monitor its data protection practices, identify any gaps or issues, and take necessary actions to maintain compliance.

6.5 By achieving these policy objectives, the college aims to protect individuals' personal data, maintain their privacy rights, and comply with the legal obligations and best practices in data protection.

7. Policy Statement

7.1 Principles:

7.1.1 *Lawfulness, Fairness, and Transparency*: We will ensure that personal data is processed lawfully, fairly, and transparently. We will provide individuals with clear and concise information about the processing of their personal data through privacy notices or other appropriate means.

7.1.2 *Purpose Limitation*: We will only collect and process personal data for specified, explicit, and legitimate purposes. We will not further process personal data in a manner that is incompatible with the original purpose for which it was collected.

7.1.3 *Data Minimisation*: We will collect and process personal data that is adequate, relevant, and limited to what is necessary for the purposes for which it is processed. We will take reasonable steps to ensure the accuracy of the personal data we hold and keep it up to date.

7.1.4 *Accuracy*: We will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date. We will rectify or erase personal data that is inaccurate or incomplete, taking into account the purposes for which it is processed.

7.1.5 *Storage Limitation*: We will retain personal data for no longer than is necessary for the purposes for which it was collected, taking into account legal, regulatory, and operational requirements. When personal data is no longer required, we will securely dispose of it.

7.1.6 *Integrity and confidentiality (Security)*: We will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage. We will regularly review and update our security measures to maintain their effectiveness as appropriate.

7.1.7 *Accountability*: We will be accountable for our data protection practices. We will maintain records of our processing activities, conduct data protection impact assessments where required, and cooperate with the Information Commissioner's Office (ICO) in the event of any data protection breach or investigation.

7.2 *Lawful bases for processing personal data*

The UK GDPR provides several lawful bases for processing personal data. The lawful bases determine the legal grounds on which Morley College London can collect and process personal data. The lawful bases for processing are as follows:

7.2.1 Consent: Processing is based on the explicit and informed consent of the data subject. Consent must be freely given, specific, informed, and unambiguous. The data subject has the right to withdraw consent at any time.

7.2.2 Contractual Necessity: Processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the data subject's request prior to entering into a contract. This basis applies when processing is required to fulfil the terms of a contractual agreement.

7.2.3 Legal Obligation: Processing is necessary for compliance with a legal obligation to which the data controller is subject. This basis applies when processing is required to fulfil legal obligations imposed by relevant laws or regulations.

7.2.4 Vital Interests: Processing is necessary to protect the vital interests of the data subject or another individual. This basis applies when processing is required to protect someone's life or physical integrity.

7.2.5 Public Task: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

7.2.6 Legitimate Interests: Processing is necessary for the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject. This basis requires a careful assessment of the legitimate interests pursued and the impact on individuals' rights and freedoms.

7.3 *Data Subject Rights*

Data subject rights refer to the individual rights granted to individuals whose personal data is being processed. Under data protection laws, including the UK GDPR, individuals have the following rights:

7.3.1 *Right to be informed*: Individuals have the right to be informed about the collection, processing, and use of their personal data. We will provide clear and concise privacy notices that outline the purposes, lawful basis, retention periods, and rights of individuals in relation to their personal data.

7.3.2 *Right of Access*: Individuals have the right to obtain confirmation as to whether their personal data is being processed and, if so, to access that personal data and obtain a copy of it. This allows individuals to understand and verify the lawfulness of the processing.

7.3.3 *Right to Rectification*: Individuals have the right to request the correction or rectification of inaccurate or incomplete personal data concerning them. If the data held by the organisation is incorrect or outdated, the individual has the right to have it corrected. For students, this could be achieved through the online enrolment platform or on person through the Student Services team. For staff, this may be able to be done using the Access People self-service platform or through the People Operations team.

7.3.4 *Right to Erasure (Right to be Forgotten)*: Individuals have the right to request the deletion or removal of their personal data when it is no longer necessary for the purposes for which it was collected, when the individual withdraws consent, when there is no legitimate interest in processing, or when processing is unlawful.

7.3.5 *Right to Restriction of Processing*: Individuals have the right to request the restriction of processing of their personal data under certain circumstances. This means that Morley College London can store the data but not process it further, typically during the resolution of a dispute or when the individual contests the accuracy of the data.

7.3.6 *Right to Data Portability*: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format. They also have the right to transmit this data to another data controller without hindrance if the processing is based on consent or contractual necessity.

7.3.7 *Right to Object*: Individuals have the right to object, on grounds relating to their particular situation, to the processing of their personal data. This includes the right to object to direct marketing, profiling, and processing for purposes of

scientific or historical research or statistical purposes, unless there are compelling legitimate grounds for the processing.

7.3.8 *Right not to be Subject to Automated Decision-Making*: Individuals have the right not to be subject to solely automated decisions, including profiling, that significantly affect them. They have the right to request human intervention and to express their point of view when decisions are made based solely on automated processing.

8 Implementation of Policy:

8.1 *Data Controller*

Morley College London is the data controller for the personal data it collects and processes. As the data controller, we determine the purposes and means of processing personal data.

8.2 *Data Protection Officer (DPO)*

Morley College London has appointed the Chief Planning and Data Officer as the College's Data Protection Officer who is responsible for overseeing compliance with data protection laws and this policy. The DPO serves as a point of contact for individuals and the ICO regarding data protection matters.

8.3 *Data Processors*

Where Morley College London engages third-party service providers to process personal data on our behalf, we will ensure that appropriate data processing agreements are in place to ensure the security and confidentiality of personal data.

8.4 *Data Subject Rights*

We recognise the rights of individuals regarding their personal data. We will respond to such requests in accordance with the applicable data protection laws.

8.5 *Policy Communication and Awareness*:

The Data Protection Policy will be communicated to all employees, contractors, and individuals involved in processing personal data within the college. This will include providing access to the policy document, conducting training sessions, and raising awareness about data protection responsibilities, principles, and best practices.

8.6 *Privacy Notice:*

The College's privacy notice is provided to individuals whose personal data is collected and processed by Morley College London This informs individuals about the purposes, lawful basis, retention periods, and their rights in relation to their personal data.

8.7 *Consent Management:*

For processing activities that require consent, Morley College London has established procedures for obtaining and managing consent from individuals. This includes ensuring that consent is freely given, specific, informed, and unambiguous. Systems are in place to record and manage consent, allowing individuals to withdraw their consent easily.

8.8 *Retention and Disposal of Data*

The College will normally keep Personal Data only for as long as it is required to retain them for legal or other statutory reasons or as required by the funding or examination body or to meet its responsibilities as an employer (for example, in relation to data

regarding pensions, taxation, potential or current disputes or litigation regarding the employment), contractor or education provider.

Personal Data will be disposed of in a way that protects the rights and privacy of Data Subjects (for example, by shredding, disposal as confidential waste or secure electronic deletion).

Morley has established 3 categories of records and retention is handled accordingly for each category:

- Category one: records required for current business purposes.
- Category two: records retained because of a statutory or regulatory requirement.
- Category three: other records retained for their historical value.

8.9 *Data Protection Impact Assessment*

The College will carry out a risk assessment in relation to the use of Personal Data for any new service, product or process. This must be done via a Data Protection Impact Assessment (DPIA): https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx.

9 Communication and Training:

9.1 We will provide appropriate data protection training to employees and other individuals involved in processing personal data on behalf of Morley College London

9.2 We will raise awareness about data protection obligations and encourage a culture of privacy and data protection.

10 Monitoring and Reporting:

10.1 We will regularly review and update this Data Protection Policy to ensure its continued effectiveness and compliance with applicable data protection laws. We will monitor our data protection practices to verify compliance and address any issues identified.

10.2 The implementation of the Data Protection Policy will be monitored by the College Risk Management Committee and the Audit Committee of the Governing Body.

10.3 For any questions or concerns regarding the processing of personal data or this Data Protection Policy, please contact our Data Protection Officer at dpo@morleycollege.ac.uk.

10.4 If you or another data subject are not satisfied with how the University is processing personal data, a complaint can be made to the Information Commissioner. You can find out more about your rights under data protection legislation from the Information Commissioner's Office website.

11 Related References, Policies, Procedures, Forms and other Appendices:

11.1 Freedom of Information Policy
11.2 Access Control Policy
11.3 Information Technology Systems Acceptable Use Policy
11.4 Social Media Policy
11.5 College Privacy Notice
11.6 Data Protection Impact Assessment template