THRIVE. ACHIEVE. EXCEL.

MONT ROSE® COLLEGE

# Data Protection Policy

## 2025 - 2027

**Approved by:** Academic/Quality Assurance Board
**Date of approval:** 19/02/2026
**Effective date:** 19/02/2026
**Next review date:** 31/03/2027

1. Mont Rose College of Management and Sciences (College) collects and processes personal data about its staff, students, and other data subjects for academic, administrative, and commercial purposes, as well as to comply with statutory obligations to the government and other statutory bodies in accordance with current data protection legislation, including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2. The College processes personal information to deliver education and support services to students and staff; advertise and promote the College and its offerings; publish the College magazine (Zypher); manage alumni relations; conduct research; and maintain our accounts and records. We also process personal information for CCTV purposes, including monitoring and collecting visual images for security and the prevention and detection of crime.

3. Personal data is protected by specific legal safeguards and regulations, which restrict how organisations process personal data. The College is responsible for ensuring adherence to the data protection requirements outlined in this policy. Failure to comply may lead to complaints, regulatory action, fines, and reputational damage.

4. This policy should be read in conjunction with the Data Quality Policy, as all staff must make every effort to ensure that any data collected or entered into our systems is accurate, valid, reliable, timely and relevant.

## Applicability and Scope

5. This policy applies to all College employees, students, contractors, other third parties, and visitors. All College staff, students, contractors, other third parties, and visitors are expected to be familiar with this policy and to comply with its terms.

6. This policy applies to all handling of personal data in electronic form, including databases, emails, and unstructured electronic documents, or stored in paper-based manual files that are organised for easy access to information about individuals.

7. It also applies regardless of where data is stored if it is being processed for College purposes, such as data on off-site and on-site systems, including on mobile devices like tablets, laptops, or phones, and regardless of who owns the device where it is stored.

8. The College is dedicated to conducting its activities in accordance with all relevant data protection laws and regulations, while upholding the highest standards of ethical conduct. This policy outlines the expected behaviours of staff and third parties

concerning the collection, utilisation, retention, transfer, disclosure, and destruction of personal data.

## Definitions

9. Personal Data refers to any information related to an identified or identifiable natural person ('data subject'). An identifiable natural person is someone who can be recognised, directly or indirectly, particularly through an identifier such as a name, an identification number, cardholder data, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

10. Sensitive Personal Data includes information relating to racial or ethnic origin, disability, political opinions, religious beliefs, trade union membership, health, sex life, and criminal convictions. The processing of sensitive personal data is subject to much stricter conditions. In certain circumstances, we would need to obtain explicit consent for this type of data and maintain robust records of that consent.

11 Processing means any operation or set of operations carried out on personal data or sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, or destroying.

12 The Data Controller is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data.

13 The Data Processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

14 'Consent of the Data Subject' means any freely given, specific, informed, and unambiguous indication of an individual’s wishes, by statement or clear affirmative action, signifying agreement to the processing of personal data relating to them.

## Data Protection Principles

15 The principles below underpin this policy and have been adopted by the College to regulate the processing of Personal Data:

a) Principle 1: Lawfulness, Fairness, and Transparency - Personal data shall be processed lawfully, fairly, and transparently concerning the data subject. This means

the College must inform the data subject about the processing (transparency), ensure the processing matches the description given (fairness), and that it serves one of the purposes specified in applicable data protection regulations (lawfulness). b) Principle 2: Purpose Limitation - Personal data shall be collected for clear, legitimate purposes and not processed further in a way incompatible with those purposes. The College must clearly specify the use of any personal data collected and limit processing to what is necessary to achieve that purpose.

c) Principle 3: Data Minimisation - Personal data shall be adequate, relevant, and limited to what is necessary for processing. The College must not keep any personal data beyond what is strictly needed.

d) Principle 4: Accuracy - Personal data shall be accurate and kept up to date. The College must implement processes to identify and correct outdated, incorrect, or redundant personal data.

e) Principle 5: Storage Limitation - Personal data shall be stored in a form that permits identification of data subjects for no longer than necessary for processing. The College should, where possible, store data in a way that limits or prevents identification.

f) Principle 6: Integrity and Confidentiality - Personal data shall be processed securely, protecting against unauthorised or unlawful processing and accidental loss, destruction, or damage. The College must apply appropriate technical and organisational measures to maintain data integrity and confidentiality.

g) Principle 7: Accountability - The Data Controller is responsible for, and must demonstrate, compliance with these principles. This requires demonstrating that the seven Data Protection Principles are applied to all personal data under their responsibility.

## Processing of Personal Data

16. The College will hold only the minimum personal data needed for its functions, and this data will be erased once it is no longer required, according to recommended retention periods.

17. Whenever feasible, personal data will be stored in one location, with a designated responsible person to support compliance, improve data security, ensure data consistency, facilitate access, and verify explicit consent for sensitive or externally transmitted data.

18. Every effort will be made to keep data accurate and current, and inaccuracies will be corrected promptly.
19. Personal data will be treated as confidential and processed in accordance with UK GDPR, the Data Protection Act 2018, and the College's notification under these laws.
20. Personal data must not be shared with unauthorised third parties unless for normal College business or legally required.
21. Both individuals and the College could face prosecution for breaches. The College will provide appropriate training and regularly review its systems and procedures.

## Responsibilities

22. As a corporate body, the College is the Data Controller. The senior officer responsible for ensuring compliance with the Data Protection Act is the Data Protection Officer.
23. The Data Protection Officer oversees the implementation of this policy in line with the Act. The current Data Protection Officer could be contacted at dpo@mrcollege.ac.uk
24. All staff and students have duties, including:
a) Processing personal data in line with this policy and guidance.
b) Complying with current Data Protection laws and principles.
c) Ensuring data subjects consent where required and understand how their data will be used.
d) Not collecting data for one purpose and using it for another without proper authorisation.
e) Not disclosing personal data outside the College without consent.
f) Not revealing data about individuals to unauthorised third parties, whether verbally or in writing.
g) Only processing data for approved purposes related to work, research, or study. h) Avoiding recording information that individuals would not want visible.
i) Securing and properly disposing of personal data.
j) Ensuring data is deleted or shredded when no longer needed.
k) Ensuring data provided during enrolment or employment remains accurate and up-to-date, and advising the College of changes.
l) Using information only for necessary purposes, retaining it only as long as needed, and following retention schedules.

m) Consulting line managers, senior management, or the Data Protection Officer if unsure about handling personal data.

n) Complying with security policies when working remotely or using mobile devices.

o) Conducting a Data Protection Impact Assessment (DPIA) for new initiatives involving personal data, with the DPIA reviewed and approved by the Data Protection Officer before implementation. (Annex A)

p) Addressing data protection queries, subject access requests, and complaints promptly.

q) Reporting any mistaken or accidental receipt of personal data immediately to the Data Protection Officer.

## Data Protection Breaches

25. Staff and students must promptly report any suspected data protection breaches to the Data Protection Officer and support resolution efforts.

26. If personal data is lost, stolen, or accidentally disclosed, it must be reported immediately to line management, IT Services, and the Data Protection Officer.

27. Anyone who believes the Data Protection Policy has been violated regarding their data should contact the Data Protection Officer at dpo@mrcolleghe.a.uk. If unresolved, they may pursue internal grievance or complaints procedures.

## Personal Data in the Public Domain

28. The College publicly shares some information about staff and students, such as on the website or in publications. 'Public domain' data is information that is already publicly available and may be shared without consent.

29. The College will publish certain data unless individuals object, including names, work email addresses, phone numbers, qualifications, biographies, and CVs of staff and Council members, where provided.

30. Processing of already publicly available personal information about third parties must comply with the Data Protection Act and should not cause harm or distress.

**Data Security**

31. The College commits to securing personal data through physical, technical, and organisational measures, including preventing loss, damage, unauthorised access, and other risks specified in the Information Security Policy.

## Data Subject Rights

32. Individuals can access personal data held by the College and may also object to processing, automated decisions, and profiling, or request data portability, correction, or deletion. Requests should follow detailed guidance.
33. The College will handle these requests lawfully, without charging, unless requests are excessive.
34. Requests must be made in writing and sent to the Data Protection Officer, who will log and ensure responses within 30 days.
35. Verification may be required to confirm identity.
36. Before starting research involving personal data, researchers and supervisors must consider this policy and guidance, especially regarding consent, secure storage, and retention.
37. Personal data for research should be minimal and, where possible, anonymised.
38. Processing sensitive or special categories of data requires explicit consent or meeting specific legal conditions, with additional protections in place.
39. Any breach or potential violation of this policy must be reported to the Data Protection Officer (DPO) at dpo@mrcollege.ac.uk, who will act accordingly and inform authorities.
40. Non-compliance may lead to disciplinary measures.

## Data Collection

41. Personal data should generally be collected directly from the data subject unless there's a justified emergency or legal necessity.
42. If data is gathered from others, the data subject must be informed unless they already have the information, confidentiality applies due to professional secrecy, or the law requires withholding information.
43. Notification to the data subject should occur promptly, within one month or at first communication.

## Data Subject Consent

44. Personal data collection must be lawful and fair, with consent obtained when appropriate.
45. A system must be established to document and manage consent, including the scope, method, date, and ability to withdraw consent.

## Data Subject Notification

46. Data subjects must be informed of processing purposes when requesting consent or collecting data, and records of disclosures should be kept.
47. External websites must include approved Privacy and Cookie notices.

## Data Processing

48. Personal data is used for daily operations and administration, adhering to ICO notifications.
49. Data use should always consider the data subject's expectations.
50. Processing must meet legal or contractual requirements, including the necessity for contract performance, legal compliance, vital interests, public interest, legitimate interests, or consent.

## Processing of Special Categories of Data

51. Special categories of data (sensitive data) will only be processed with express consent or under specific legal conditions, such as legal obligations or protecting vital interests.
52. Additional security measures are required, including prior approval and clear documentation.

## Data Quality

53. The College will ensure that personal data is accurate, complete, and regularly updated.

## Profiling and Automated Decision-Making

54. Engagement in profiling or automated decisions will be limited to contract-related or legally authorised activities, with disclosures provided to data subjects.

## Digital Marketing

55. Personal data must not be used for promotional marketing without prior consent.
56. Data subjects will be informed of their right to object at the time of first contact. 57. Withdrawals of consent must be respected immediately, with details recorded for compliance.

## Data Retention

58. Data will only be kept as long as necessary to fulfil its original purpose or further processing purposes.

59. Retention periods are outlined in relevant policies, and data will be securely deleted when no longer needed.

## Information Security and Data Protection

60. The College will implement measures to secure personal data against risks by regularly managing information security and data protection risk register and reporting to the Audit Committee.

## Data Subject Requests

61. Procedures will be established to facilitate rights related to access, objection, restriction, erasure, rectification, and data portability.

62. Requests will be considered lawful without fees unless deemed excessive.

63. Data subjects have the right to ask the College to correct or supplement inaccurate, misleading, outdated, or incomplete personal data, and they are entitled to access the following information about their own personal data:

a) The purposes of the collection, processing, use, and storage of their personal data.

b) The source(s) of the personal data if it was not obtained from the data subject;

c) The categories of personal data stored for the data subject.

d) The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the locations of those recipients.

e) The intended duration of storage for the personal data or the reasoning behind the storage period.

f) The use of any automated decision-making, including profiling.

g) The rights of the data subject (where applicable) to:

i. Object to the processing of their personal data.

ii. Lodge a complaint with the Data Protection Authority (i.e. Information Commissioner's Office).

iii. Request the rectification or erasure of their personal data.

iv. Request the restriction of processing of their personal data.

64. It is preferred that requests for access to or correction of personal data be made in writing; however, they can also be made verbally or via social media. Any staff

member who receives such a request must forward it to the Data Protection Officer, who will record the details of the request. Verification must confirm that the requester is either the data subject or their authorised legal representative. A response to each request will be provided within 30 days of receipt of the data subject's written request.

65. If the College is unable to respond fully within 30 days, the Data Protection Officer will nonetheless provide the following information to the data subject or their authorised legal representative within the specified timeframe:

a) An acknowledgement of receipt of the request.

b) Any information located to date.

c) Details of any requested information or modifications that will not be provided, along with the reasons for the refusal and any procedures available for appeal.

d) Remaining responses will be provided within two months of the original end date.

e) An estimate of any costs payable by the data subject (e.g., where the request is excessive).

66. It should be noted that there may be cases where fulfilling the data subject's request would disclose personal data about another individual. In such circumstances, information must be redacted or withheld as necessary or appropriate to protect that person's rights.

## Data Protection in Law Enforcement

67. Personal data can be shared without consent if necessary for crime prevention, prosecution, taxation, or court orders, with limits on processing when it could prejudice investigations.

68. Requests from authorities must be promptly reported to the Data Protection Officer for guidance.

## Transfers to Third Parties

69. Personal data will only be shared with third parties when assured it will be processed lawfully and securely. Agreements will specify responsibilities, including Data Sharing Agreements or Processing Agreements, depending on whether the third party is a controller or processor.

70. Regular audits of third-party processing will be conducted, and deficiencies addressed.

71. Data transfers outside the UK are permitted if the destination country provides adequate legal protection or if lawful mechanisms are employed.
72. Complaints should be directed in writing to the Data Protection Officer at dpo@mrcollege.ac.uk
73. Non-compliance with this policy may lead to disciplinary action.

## Complaints Handling

74. Data subjects with a complaint about the processing of their personal data should put the matter forward informally in writing to the Data Protection Officer at dpo@mrcollege.ac.uk. An investigation of the complaint will be carried out to the extent appropriate, based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and outcome of the complaint in accordance with the College's Internal Review Procedures.
75. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their discretion, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office.

## Breach Reporting

76. Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer, describing what occurred. Notification of the incident can be made via dpo@mrcollege.ac.uk or by calling 02085565009.
77. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the incident protocols.

## Responsibilities

78. The Data Protection Officer is accountable for the implementation of this policy in the College and will be responsible for:
a) Keeping the data risk register updated.
b) Reviewing all data protection procedures and policies on a regular basis.
c) Arranging data protection training and advice for all staff members and those included in this policy.

d) Answering questions on data protection from staff, board members and other stakeholders.

e) Responding to individuals such as clients and employees who wish to know which data is being held on them by the College.

f) Checking and approving third parties that handle the company's data, any contracts or agreements regarding data processing.

g) Ensure all systems, services, software and equipment meet acceptable security standards.

## Data Protection Training

79. All College employees who have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. The College will provide regular data protection training and procedural guidance for staff.

## Data Protection by Design

80. To ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

81. Each department must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Officer, for all new and/or revised systems or processes for which it has responsibility. (Annex A).

82. The subsequent findings of the DPIA must then be submitted to the Data Protection Officer for review and approval. Where applicable, the DTS Directorate will assess the impact of any new technology use on the security of personal data