THRIVE. ACHIEVE. EXCEL.

MONT ROSE® COLLEGE

Data Protection Policy

2023 – 2025

Approved by: Academic/Quality Assurance Board
Date of approval: 31/05/2023
Effective date: 31/05/2023
Next review date: 31/05/2025

Policy intent

Mont Rose College is dedicated to operating in compliance with all relevant data protection laws and rules at the highest ethical standards. The expectations for Staff and external parties and students are outlined in this policy with regard to the gathering, use, retention, transfer, disclosure, and destruction of any personal data.

This policy applies to all personal data and sensitive data collected and processed by Mont Rose College of Management and Sciences in the code of conduct of its business, in electronic in any medium, and within paper filing.

Organisations' Personal data processing is subject to legal safeguards and other standards that limit how personal data may be used. The College is responsible for ensuring compliance with the guidelines outlined in this policy for data protection. Failure to comply could subject the College to criticism, legal repercussions, penalties, and/or reputational harm.

Definitions and Terminology

- **Consent** is any freely given, specific, informed, and unambiguous indication of the data subject's wishes. This is done by a statement or a clear affirmative action, signifying agreement to the Processing of personal data relating to them.

- **Processing** refers to any action taken, individually or in combination, on an individual's or an individual's set of data, whether or not that action is carried out automatically. Examples include gathering, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or other availability, alignment or combination, restriction, erasure, or destruction.

- **Personal data** is any information pertaining to a named, recognisable, or locatable individual (a "data subject") that is considered personal data. An identifiable natural person is one who can be located, directly or indirectly, especially with reference to an identifier like a name, identification number, location information, online identifier, or one or more characteristics unique to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity.

- **Sensitive Personal Data** is information about a person's racial or ethnic background, physical or mental impairment, political or religious beliefs, union membership, health, sexual preferences, and criminal convictions are considered sensitive personal data. Sensitive personal data handling is governed by tougher rules. For this kind of data, it is anticipated that we would need to obtain explicit authorization and maintain thorough records of this consent.

Data protection principles

Mont Rose College has adopted the following principles to regulate the way in which personal data is processed:

- **Principle 1: Lawfulness, Fairness, and Transparency -** Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject. This means the College is required to tell the data subject what Processing will occur to ensure transparency, the Processing must match the description given to the data subject to ensure fairness, and it must be for one of the purposes specified in the applicable data protection regulation according to the lawfulness.

- **Principle 2: Purpose Limitation -** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in an incompatible manner. To ensure this, the College must specify exactly what the personal data collected will be used for and limit the Processing of that personal data to only what is necessary to meet the specified purpose.

- **Principle 3: Data Minimisation -** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Therefore the College will not store any personal data beyond what is strictly required.

- **Principle 4: Accuracy-** All personal data shall be accurate and kept up to date. The College shall ensure this by having a process in place for identifying and addressing out-of-date, incorrect, and redundant personal data.

- **Principle 5: Storage Limitation-** Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. The College ensures, wherever possible, stored personal data is done in a way that limits or prevents identification of the data subject.

- **Principle 6: Integrity and Confidentiality-** Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage. The College ensures appropriate technical and organisational measures are carried out to ensure the integrity and confidentiality of personal data are maintained at all times.

- **Principle 7: Accountability-** The College will demonstrate that all six data protection principles are abided by in regard to all personal data it is responsible for. The data protection officer is responsible for and should be able to demonstrate compliance on behalf of the College.

Policy provisions

Data Breach

- A data breach is any security incident in which unauthorised parties gain access to sensitive data or confidential information, including personal data (contact details, bank account numbers, etc.) or corporate data (Student/staff data records, intellectual property, financial information).

- In the event that you may think a data breach has taken place, the Data Protection Officer (DPO) must be informed immediately with a description of what occurred. Notification of the breach can be made via email DPO@mrcollege.ac.uk or by phone call 020 8556 5009

- The DPO will then investigate and will assess as soon as possible the nature and severity of the breach. Depending on the severity, the DPO will do the following;

    - Low risk: If there is no risk of harm to the Data Subject, the DPO will record the breach in the Data risk register, and the person who breached is required to complete a Data protection refresher course.

    - High risk:
        - The DPO will ensure robust breach detection, investigation, and internal reporting procedures in place.
        - A report to ICO and those affecting individuals within 72 hours
        - Report the incident in the Data risk register.
        - Those who caused the breach will be required to carry out a Data protection refresher course.
        - Comply with any requirements of the ICO.

Processing and collecting personal data

- Individuals will be informed that their information has been collected, and the intended use of the data will be disclosed either at the time of collection or at the earliest opportunity after collection. Personal information will only be gathered and processed as needed to meet the College's needs or legal requirements.

- To be in compliance with the data protection legislation, manual or computerised personal data will be stored in a single location with a named responsible person whenever possible. Improved data security, consistent data sets, user-friendliness, and confirmation of specific (written) authorization for sensitive data.

- All precautions will be taken to guarantee that the information is accurate and current and that inaccuracies are fixed without excessive delay. Data collected

shall be erased once the need to retain the information has passed in accordance with the recommended retention period.

- Violations of the Data Protection Act 2018 (DPA) could possibly leave both the individual and the College open to possible legal action. The College will examine its system and processes following this evaluation and will take all reasonable measures to offer training and advice on the use of personal data.

- Staff will advise the Data Protection Officer in the event of any intended new purposes for processing personal data. The DPO may then arrange for a Data Protection Impact Assessment to be conducted.

Responsibilities

The data protection officer is the senior officer responsible for ensuring that the College is compliant with the Data Protection Act and ensuring that the Data Protection Act's guidelines are followed in the execution of the Data Protection Policy. The data protection officer is Rezime Orife DPO@mrcollege.ac.uk.

All Staff and Students are responsible for ensuring:

- All Staff should have a clear desk policy; this means at the end of the working day no documents should be left on the table. Personal data should be locked away in drawers or cupboards.

- Processing of personal data is done in accordance with the Colleges Data Protection Policy and Data protection act and the Data Protection Principles.

- Data subject involved has given their consent and is aware of how the data given is being used.

- Personal data will not be disclosed to a third party outside of the College without the consent of the data subject.

- Personal data relating to data subjects is only ever processed for approved work, research, or study-related purposes.

- Data subjects have the right to access their personal information, comments, or other information about them that they would feel uncomfortable with the other person knowing is not kept on file in emails or anywhere else.

- Information is disposed of correctly, making sure that it is permanently removed from servers and that hard copies of information are confidentially shredded and not disposed of in a wastepaper basket/recycle bin.

- Any information given to the College in connection with their enrollment or employment is true and current, and they agree to quickly notify the College of any changes to their personal information (such as an address change or change in emergency contact information).

- If there is any uncertainty regarding how to handle personal data, line managers, senior management, or the data protection officer are consulted.

- They are familiar with and comply with the College's staff handbook stating the code of conduct relating to the use of Mobile Data Devices Use if they are working remotely or using a mobile device to store data (for example, a laptop, tablet, or mobile phone).

- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to Data Protection Officer.

- Any personal information obtained accidentally, regardless of how is notified to the Data Protection Officer immediately and handled by the relevant College employee.

- Staff and students must ensure that any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that they support the Data Protection Officer in resolving breaches.

- If an individual finds any lost or discarded data that they believe contains personal data (for example, a memory stick), they must report the matter to their line manager/ lecturer and report it to the Data Protection Officer immediately.

- An individual must notify their line manager and the data protection officer as soon as they learn that personal data has been unexpectedly lost, stolen, or inadvertently revealed (for instance, if their laptop or phone holding personal data is misplaced).

- Any employee or student who believes the Data Protection Policy has not been followed with regard to personal information about them should first bring up the issue with the Data Protection Officer or HR Services Director. Students and employees can turn to the Student Complaints Procedure or the Employees Grievance Procedure, respectively, if the issue cannot be handled amicably.

Personal Data within the Public Domain

- The College retains some information about its employees and students in the public domain, such as on its website or in publications. 'Public domain' refers to information that is already in the public domain and can be shared with other parties without the data subject's consent.

- Certain amounts of personal information, such as names, workplace emails, phone numbers, academic credentials, biographies, and curriculum vitae of Academic Staff, support staff, and Council members, will be made public by the College unless the individual objects.

- The College may process personal data on third parties already in the public domain if the Processing complies with the Data Protection Act's principles and is unlikely to result in the data subject experiencing harm or distress.

Data security

- The Data Protection Act mandates that personal data is kept safe. As a result, all staff members are accountable for being aware that:
    - To safeguard personal data in paper or hard copy shall be kept locked away locked in filing cabinets, drawers, and offices.
    - To safeguard electronic data the following will be used were necessary :
        - Password protection
        - Locking of desktops/laptops when left unattended
        - Any portable devices (e.g., memory sticks) on which personal data is stored are encrypted, kept in a secure location, and transferred from one place to another with care to avoid accidental loss.
        - Mobile devices used to access or store personal data are properly password protected and, where appropriate, encrypted.
    - Relevant Data Protection Awareness Training will be provided to Staff to keep them better informed of relevant legislation and guidance regarding the Processing of personal information. Data protection training will also promote awareness of the College's data protection and information security policies, procedures, and processes. Staff are strongly encouraged to complete this training during induction and subsequently on an annual basis.
    - There are measures, for instance, to restrict access to email communications to intended recipients of the College and their suppliers and measures to ensure the storage facility of your personal information is safe. However, given the fact that the Internet is not an entirely secure medium and, therefore, not completely free from risks, it is acknowledged that, as is the case with any other website, the absolute privacy of personal information cannot be guaranteed.

Rights to Access Information

- Everyone within our community has the right to view the personal information that the College may have about them. Additionally, they have the right to object to Processing, decision-making, and profiling. As well as restrict Processing, the right to data portability, correction, and deletion. The Detailed Guidance section should be read by anybody who wants to exercise these rights.

- In compliance with all relevant Data Protection rules and regulations, the College will take requests pertaining to any of the previously mentioned rights under consideration. For taking into account and granting such a request, no

administrative fee will be imposed unless the request is considered to be excessive in scope.

- The Data Protection Officer must receive all written requests to access or rectify personal data. The Data Protection Officer will document each request as received and ensure the proper departments react to requests.

- According to the proper verification, the requestor must be the data subject or their approved legal representative. Each request will receive a response within 30 days of the data subject's written request.

Internal communication

- Mont Rose College of Management and Sciences uses electronic mail to communicate official Mont Rose College information of many kinds to Staff, Students, and others. Staff are responsible for reading and responding to their email on a frequent and regular basis since some official communications may be time-sensitive. Mont Rose College of Management and Sciences suggests that Staff access their email account on a daily basis. Staff needs to set up an automatic out-of-office reply through Gmail when they are away from the College. This should include alternative contact details for urgent inquiries.

- All users of the college email service must abide by the following conditions :
    - No user should send insulting, abusive, bullying, harassing, obscene, racist, sexist, offensive, or incitement to commit a criminal offense or threatening or which may contain any malicious code; for example, virus

    - No information should be communicated within or outside the College, which is defamatory, brings Mont Rose College into disputes, or violates laws.

    - All users must act sensibly and appropriately when using the College's email or computing facilities to send an email, whether internally or externally, using the Internet.

- Students' Personal email addresses may be used to contact them in specific instances; the main way of contact will be via college email.

Enforcement

- Any violation of this policy, whether actual or suspected, must be reported through email to the data protection officer. In addition to taking the necessary measures, the data protection officer will notify the relevant internal and external authorities.
- Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

Detailed Guidance

Data collection

- Only the data subject should provide personal information unless one of the following situations occurs:
    - The collection must be done urgently in order to safeguard the data subject's vital interests or to stop substantial loss or harm to another person.
    - Personal data from other persons or bodies should be collected because of the business purpose.

- The data subject must be notified of the gathering of personal data if it comes from someone other than them unless one of the following situations occurs:
    - The required information was provided to the data subject by other means.
    - Due to a professional confidentiality requirement, the knowledge must be kept private.
    - The gathering, Processing, or transfer of personal data is specifically permitted under national legislation.

- When it has been decided that a data subject has to be notified, this should happen immediately; however, there is up to one calendar month after the initial collection, the initial communication, or the initial disclosure.

Data subject consent

- The College will only collect personal information about individuals through authorised and ethical methods and, when necessary, with that person's knowledge and consent.

- The College follows the following procedure when gaining consent from data subjects before collecting, using, or transferring their personal information. The system must provide the following provisions:

    - Consideration of which disclosures are required in order to obtain valid consent

    - Guarantee the request for consent is presented in a fashion that is clearly distinguished from other matters. This shall be made in a form that is understandable and accessible and embodies clear and simple language.

    - Ensuring that consent is freely provided (i.e.not, dependent on a contract that requires the Processing of personal data that is unnecessary for the performance of that contract).

    - Recording the date, manner, and details of the information disclosed and the legality, extent, and preferred format of the consent granted.

- Offering a data subject a simple method to withdraw their permission at any moment

Data subject notification

The College shall inform data subjects of the reason why their personal data is being processed. All necessary disclosures will be made verbally, electronically, or in writing when the data subject is sought to consent to Processing personal data or when any personal data is obtained from the data subject. Along with a record of the facts, date, content, and manner of disclosure, the accompanying form should also be kept.

The College's external website provides a 'privacy notice' and an online 'cookie notice' fulfilling the requirements of applicable law, which is also approved by the data protection officer prior to publication.

Data processing

- According to the information provided in the notice to the Information Commissioner's Office, the College uses personal data for the general management of the organisation and business administration.
- A data subject's perspective should always be considered when using their information to determine if the usage will align with their expectations or whether they are likely to object.
- The College will only handle personal data if at least one of the following conditions is satisfied. The College will treat personal data in compliance with all relevant laws and applicable contractual commitments:
    - The individual whose personal data is being processed has granted permission for it to be done so for one or more defined reasons.
    - Processing is required to fulfil obligations under a contract to which the data subject is a party or to carry out actions at the subject's request before finalising a contract.
    - Processing is required to fulfil the obligations that the data controller must comply with by law.
    - Processing is essential to safeguard the subject's or others' vital interests.
    - Processing is required to carry out a duty in the public interest or in order to exercise the data controller's official authority.
    - Processing is required to further the legitimate interests of the data controller or a third party unless those interests are outweighed by the interests of the data subject or by their basic rights and freedoms, particularly if the data subject is a child.

- There are various circumstances in which the College will consider the additional requirements listed below in any situation where consent has not been obtained for the specific Processing in order to assess the fairness and transparency of any processing that goes beyond the original purpose for which the personal data was collected:
    - If there is a connection between the purpose for the personal data collected and the reason for further Processing.
    - The circumstances surrounding the collection of personal data, particularly with regard to the relationship between the data subject and the data controller.
    - The type of personal data being processed, particularly special data categories or information on criminal convictions and crimes, are being handled.
    - Appropriate safeguarding in relation to further Processing will be put in place such as encryption, anonymization or pseudonymisation.

Processing of Sensitive data

- The College shall only process sensitive data when the data subjects have given explicit consent to the Processing or if one of the following conditions apply:
    - The Processing involves personal information that the data subject has previously made public.
    - The Processing is crucial to establish, exercising, or defending legal claims.
    - The Processing is expressly permitted or mandated by law.
    - When the data subject is physically or legally unable to give permission, the Processing is required to safeguard the vital interests of the subject or another person.
    - Additional terms and conditions, such as restrictions based on government legislation, are connected to the Processing of genetic data, biometric data, or health data.
- The College will take additional precautions where sensitive data is being processed. For instance, prior authorisation must be sought, and the rationale for the Processing must be explicitly documented together with the relevant personal data.
- The Processing of personal data cannot be consented to by children. The person who has parental responsibility for the child must provide their consent.

It should be highlighted; nonetheless, that agreement from the child or the adult who has parental responsibility is not required when Processing is permitted on other legal bases.

Profiling and Automated Decision-making

- The College will utilize automated decision-making and profiling where it is required to enter into or conduct a contract with the data subject or when it is permitted by law. When the College utilizes automated decision-making and profiling, the relevant data subjects will be notified formally.

Digital Marketing

- The College will not distribute advertising or direct marketing materials to a data subject via digital means, including email, the Internet, or mobile phones, without first getting their permission.

- When processing personal data for digital marketing purposes is approved, the data subject must be made informed from the beginning that they have the right to object to the Processing of their data for those purposes at any time.

- If data subjects express an objection in relation to digital marketing, their personal data must be ceased immediately. Their information will be kept on a suspension list with a record of their choice to opt-out.

Data Retention

- Personal data shall not be kept by the College for longer than is required in regard to the reasons for which it was initially acquired or for which it was subsequently processed in order to guarantee fair Processing.

- The College's Record Management Policy specifies how long the College must keep personal data on file. This takes into consideration the contractual and legal obligations that have an impact on the retention periods specified in the schedule. Any personal data that has been determined to be no longer necessary to keep should be removed or destroyed from all forms of storage appropriately as soon as practicable.

Information Security and Data Protection

- The College will implement organisational, technological, and physical safeguards to guarantee the privacy of personal information. This includes preventing loss or damage, unauthorised access, Processing, and other dangers to which it may be subject to human activity or the physical or natural environment.

Data Subject Request

- The College will establish a series of processes to make it possible for data subjects to exercise their legal rights with regard:
    - Data erasure

- Data portability
- Data rectification.
- Information access
- Objection to automated decision-making and profiling
- Objection to Processing
- Restriction of Processing

- In compliance with all relevant data protection laws and regulations, the College will consider requests from individuals about any of the aforementioned rights. There will not be an administration fee assessed for taking into account and/or fulfilling such a request unless it is considered to be excessive or unwarranted.

- Data subjects are entitled to request the correction of any inaccurate, deceptive, out-of-date, or incomplete personal data as well as to request the following information on their own personal data :

    - The reason for the collection, Processing, use, and storage of their data
    - If the information did not come directly from the data subject, the source(s) it came from
    - The type of personal data stored for the data subject
    - The recipients or categories of recipients to whom the personal data has been or may be transmitted, along with the location of those recipients
    - The time frame for keeping personal data on file or the reason for doing so.
    - The use of any automated decision-making, including profiling.
    - Data subjects have the right to:
        - Object to the Processing of their personal data
        - Make a complaint with the Data Protection Authority (i.e., Information Commissioner's Office)
        - Request the correction or deletion of their personal data.
        - Request restriction to the Processing of their personal data

- The Data Protection Officer must receive all requests for access to or rectification of personal data in writing, and they will record each request as it is made. According to the proper verification, the requestor must be the data subject or their authorised legal representative. Each request will receive a response within 30 days of the data subject's written request being received.

- Suppose the College is not able to respond to the request within 30 days. In that case, The Data Protection Officer is obliged to provide the following

information to the data subject or their authorised legal representative within the time frame given:

- And the acknowledgment of the request
- Any readily available information to date
- Information on the modifications requested or information that will not be given to the data subject, the reason(s) for the refusal, and any appeals processes that may be available.
- An estimated date shall be given for when the remaining information will be provided
- An estimated cost that the data subject will be responsible for covering (for instance, if the request is excessive in scope).
- The name and contact information of a college employee who the data subject should get in touch with to follow up.

- It should be highlighted that there may be circumstances in which giving the information requested by a data subject might reveal personal information about someone else. To safeguard that person's rights in these situations, the material must be restricted or withheld as may be required or appropriate.

Law enforcement requests and disclosure

- Personal information may occasionally be disclosed without the data subject's acknowledgment or consent. This is the situation when disclosing personal information is required for any of the following reasons:
  - Any detection or prevention of crime
  - The apprehension or prosecution of offenders.
  - The assessment of assessing or collection of taxes or duties
  - By any legal regulation or order of a court

- If the College deals with personal data for one of the aforementioned reasons, it may deviate from the processing guidelines in this policy, but only to the extent that not doing so would likely harm the situation at hand.

- Suppose a member of Staff within the College receives a request from law enforcement authority, courts, or regulators regarding information relating to a data subject. The Data Protection Officer must be made aware immediately so they can provide extensive support and assistance.

Transfers to Third parties

- The College will only give access to or transfer personal data to third parties (including cloud computing services) where it is certain that the recipient will use the data lawfully and safeguard it appropriately. When third-party Processing occurs, the College will first determine whether the third party is a data controller or a data processor of the personal data being transferred according to applicable law.

- Suppose the Third Party is identified as a data controller. In that case, the College will negotiate an Information Sharing Agreement with the Controller to specify each party's obligations with regard to the transmitted personal data.

- Suppose the Third Party is deemed to be a data processor. In that case, the College will enter into an adequate processing agreement, in the form of the Mont Rose College Data Processing and Information Security Agreement, with the data processor to ensure that the data processor implements the proper organisational and technical safeguards to protect the personal data.

- The College will routinely evaluate how third parties process personal data, paying particular attention to the technical and organisational safeguards they have in place. Any significant flaws found will be disclosed to the Information Commissioner's Office (ICO)

Complaints handling

- Data subjects should write to the Data Protection Officer with any concerns or complaints regarding the Processing of their personal data. Depending on the basis of the particular situation, the complaint will be investigated to the extent deemed necessary. Within a reasonable amount of time, the data protection officer will update the data subject on the status and resolution of the complaint.

- Data subjects are at liberty to resolve issues through the listed means below if they believe they cannot be resolved with the Data Protection Officer through a consultation:
    - Arbitration
    - Binding
    - Filing a complaint with the Information Commissioner's Office
    - litigation
    - Mediation

Data Protection Training

- The obligations under this policy will be explained to all College employees who have access to personal data as part of their staff induction training. Employees will receive regular training on data protection procedures from the College on an annual basis.

Data Protection Design

- The guarantee all the data protection requirements are identified and considered in the design when reviewing or expanding new systems or processes and/or existing systems or processes. All must go through an approval process before proceeding.

- The Data protection officer and relevant department staff must ensure that the Data Protection Impact Assessment is carried out for every new or revised process.