Data Protection Policy

Ownership Details and Review Schedule of Policy

Effective from	21 April 2026
Review cycle	Annual
Next Review Due Date	21 April 2027
Policy owners	Data Protection Officer
Approving Body	Board of Governors
Lead Contact	Data Protection Officer
Applicable to	This policy applies to all staff, governors, students, applicants, alumni where applicable, contractors, consultants, agents, volunteers, visitors, placement providers, partners, suppliers and any other individuals or organisations who process personal data on behalf of, or in connection with, SIRM College.
Relevant/Applicable OfS Conditions of Registration/requirements	Condition E2: Management and governance Condition F3: Provision of information to the OfS, where personal data is used in regulatory reporting or information returns Condition B3: Student outcomes, where personal data is used to monitor continuation, completion and progression Condition B4: Assessment and awards, where personal data is used in assessment, moderation, academic records, appeals or awards processes Condition E6: Harassment and sexual misconduct, where personal data is processed in relation to reports, investigations, support or casework Condition E10: Sub contractual arrangements, where personal data is processed in connection with subcontracted or partnership delivery
Other relevant / applicable legislation/requirements	UK General Data Protection Regulation, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 where applicable, the Equality Act 2010, the Counter-Terrorism and Security Act 2015 where applicable to Prevent-related processing, the Higher Education and Research Act 2017, ICO guidance and statutory codes of practice, the OfS regulatory framework and reporting requirements, HESA / Jisc collection notices and data protection requirements where applicable, and awarding body and validating partner requirements where applicable.

Data Protection Policy

DOCUMENT CONTROL

Date	Review & Revision	Owner	Version

Data Protection Policy

Table of Contents

1. Policy Statement 4
2. Data protection principles 5
3. Status and scope of the policy 6
4. Key definitions 6
5. Fair and lawful processing 8
6. Transparency 10
7. Purpose limitation 10
8. Data minimisation 10
9. Accuracy 11
10. Storage limitation and data retention 11
11. Security, integrity and confidentiality 12
12. International transfers 14
13. Data subject rights and requests 14
14. Automated processing and automated decision-making 16
15. Direct marketing 16
16. Personal data breaches and notification 17
17. Training and awareness 18
18. Records and documentation 18
19. Monitoring and review 19

1. Annex 1: Subject Access Request Procedure 21

1. Policy Statement

1.1. Individuals have legal rights over how their personal information is used. In the course of its activities, Numerica Risk Information Management Ltd, trading as SIRM College, collects, uses and stores personal information about staff, students, applicants, alumni where applicable, governors, contractors, consultants, agents, partners, suppliers, visitors and other contacts. SIRM College recognises its responsibility to handle that information lawfully, fairly, transparently and securely.

1.2. The categories of personal information SIRM College may process include details about current, former and prospective students, applicants, staff, governors, contractors, consultants, agents, partners, suppliers and other individuals it interacts with. This information may be stored on paper, in electronic systems, in cloud-based platforms, in emails, in shared drives, in student records, staff records, assessment records, complaints and casework records, safeguarding or Prevent records, admissions and recruitment records, marketing records, financial records, governance records, or in other formats.

1.3. Personal data is protected by the UK General Data Protection Regulation, the Data Protection Act 2018 and related UK data protection legislation, which set out how personal information may be used. SIRM College is committed to processing personal data in line with these requirements and expects all staff and others working on its behalf to comply with this policy and associated procedures.

1.4. This policy sets out SIRM College's institutional approach to data protection. It should be read alongside SIRM College's privacy notices, which provide more specific information to individuals about how their personal data is used in particular contexts, including applicant and student processing, staff processing, website and cookies, marketing and recruitment, online learning platforms, recorded sessions, complaints, safeguarding, Prevent, student support and other casework processes.

1.5. Where any third party handles personal data for or on behalf of SIRM College, appropriate measures will be taken to ensure that they meet equivalent standards of data protection. This includes, where relevant, awarding bodies, validating partners, agents, placement providers, professional advisers, consultants, IT providers, cloud service providers and other suppliers or processors.

1.6. SIRM College has appointed an internal Data Protection Officer. The Data Protection Officer provides independent advice, monitoring and challenge in relation to SIRM College's compliance with data protection requirements. Operational support may be provided by the Compliance team or another nominated operational lead, but this does not remove or reduce the independent oversight role of the Data Protection Officer.

1.7. This Data Protection Policy is a non-contractual document and may be updated or withdrawn at any time through SIRM College's approved governance processes. Breaches of this policy may be treated as a disciplinary matter and may also result in other action where appropriate, including action under student, contractor, supplier, agent or partner procedures.

2. Data protection principles

2.1. Anyone who handles personal data on behalf of SIRM College must comply with the following data protection principles. Personal data must be:

2.1.1. processed lawfully, fairly and in a transparent manner;
2.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
2.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is processed;
2.1.4. accurate and, where necessary, kept up to date;
2.1.5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed;
2.1.6. processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using suitable technical and organisational measures;
2.1.7. not transferred outside the UK unless appropriate safeguards are in place and the transfer complies with data protection law; and
2.1.8. processed in a way that upholds the rights of data subjects.

2.2. SIRM College is accountable for compliance with these principles and must be able to demonstrate that it meets them.

2.3. Staff and others who process personal data on behalf of SIRM College must follow this policy, associated procedures, privacy notices, retention requirements, information security requirements and any instructions issued by the Data Protection Officer or other authorised staff.

3. Status and scope of the policy

3.1. This policy sets out SIRM College's approach to data protection and the standards which must be followed when personal data is collected, used, stored, shared, accessed, transferred, retained, transported, archived, destroyed or otherwise processed.

3.2. The policy applies to all staff and workers, including employees, agency workers, contractors, consultants, volunteers and interns, and to any other individuals who have access to personal data on behalf of SIRM College, regardless of location, campus, system, format or medium.

3.3. This policy also applies, where relevant, to governors, students, applicants, alumni, agents, partners, placement providers, suppliers and other third parties who process personal data for or on behalf of SIRM College, or who are required to comply with SIRM College's data protection requirements.

3.4. SIRM College has appointed an internal Data Protection Officer who is responsible for providing independent advice, monitoring and challenge in relation to data protection compliance. The Data Protection Officer must be involved in a timely manner in matters relating to the protection of personal data, including higher-risk processing, Data Protection Impact Assessments, personal data breaches, complex Subject Access Requests, data sharing arrangements, use of data processors and any matter that may create regulatory, legal or reputational risk.

3.5. Operational coordination may be undertaken by the Compliance team or another nominated operational lead. This may include maintaining data protection logs, coordinating Subject Access Requests, gathering evidence, tracking training completion, supporting breach documentation, maintaining records and escalating matters to the Data Protection Officer where required.

3.6. Staff should raise any questions or concerns about data protection with their line manager, the Compliance team, the nominated operational lead or the Data Protection Officer in the first instance.

3.7. Anyone who believes that this policy has not been followed in relation to their own personal data, or the personal data of someone else, should report their concerns without delay to their line manager, the Compliance team, the nominated operational lead or the Data Protection Officer.

4. Key definitions

4.1. **Personal Data**, referred to as "data" in this policy, is any information relating to an identified or identifiable living individual. An individual can be identified directly or indirectly, for example through a name, identification number, student number, staff number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data can include factual information, such as contact details, attendance records, assessment records or financial records, and opinions, such as performance comments, academic judgement, complaint records or casework notes.

4.2. **Data Subjects** are the living individuals whose personal data is processed by SIRM College. They may include, for example, students, applicants, alumni, staff, governors, contractors, consultants, agents, partners, suppliers, visitors, complainants, witnesses, emergency contacts or other individuals whose personal data is processed in connection with SIRM College's activities. A data subject does not have to be a UK national or resident.

4.3. **A Data Controller** is the organisation or person that determines the purposes and means of processing personal data. SIRM College acts as Data Controller for the personal data it uses in connection with its activities, except where another organisation determines the purposes and means of processing.

4.4. **A Joint Controller** arrangement may arise where SIRM College and another organisation jointly determine the purposes and means of processing personal data. Where joint controller arrangements apply, SIRM College will ensure that responsibilities are appropriately documented.

4.5. **Data Users** are members of staff or others working for or on behalf of SIRM College whose roles involve accessing or handling personal data. Data Users must protect the data they work with and follow this policy and all related data protection and information security procedures.

4.6. **Data Processors** are organisations or individuals, other than SIRM College staff, who process personal data on behalf of SIRM College. Examples may include providers of IT systems, cloud services, student record systems, virtual learning environments, mailing services, payroll services, outsourced functions, consultants or other suppliers who handle personal data on SIRM College's behalf.

4.7. **Processing** is any activity involving personal data, whether automated or not. It includes obtaining, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, transmitting, disseminating, sharing, combining, restricting, erasing or destroying personal data, as well as making it available to others.

4.8. **Special Category Data** is a subset of personal data that is more sensitive and therefore needs higher protection. It includes data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, disability-related data, and data concerning a person's sex life or sexual orientation.

4.9. **Criminal Offence Data** is personal data relating to criminal convictions and offences, allegations of criminal activity, criminal proceedings, or related security measures.

4.10. A **Personal Data Breach** is any incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, or any compromise of the security, confidentiality, integrity or availability of that data or its protective measures. This may include, for example, misdirected emails, loss of paper records, unauthorised access to systems, incorrect sharing permissions, cyber incidents, loss or theft of devices, or accidental disclosure of information.

4.11. A **Subject Access Request** is a request from an individual for access to their personal data. A request does not need to use the words "subject access request" and may be made verbally or in writing.

4.12. A **Data Protection Impact Assessment** is an assessment used to identify and reduce data protection risks before SIRM College begins processing that is likely to result in a high risk to individuals' rights and freedoms.

5. Fair and lawful processing

5.1. Data protection law does not prevent SIRM College from using personal data, but requires SIRM College to do so fairly, lawfully and in a way that respects individuals' rights. Individuals must be informed about how their data will be used, who controls it, the lawful basis for the processing, and with whom it may be shared. This will usually be done through privacy notices and other relevant communications.

5.2. Personal data may only be processed where at least one lawful basis applies. The lawful bases that SIRM College may rely upon include:

- performance of a contract, for example a student contract, employment contract or supplier contract;
- compliance with a legal obligation;
- legitimate interests pursued by SIRM College or a third party, provided these are not overridden by the data subject's interests, rights or freedoms;
- protection of someone's vital interests;
- performance of a task carried out in the public interest, where applicable; and

- the data subject's consent.

5.3. SIRM College will identify and record an appropriate lawful basis for each processing activity. Consent will only be relied upon where it is appropriate to do so and where it can be shown that consent is freely given, specific, informed and unambiguous. Where SIRM College relies on consent, individuals must be able to withdraw consent easily at any time.

5.4. Where SIRM College relies on legitimate interests as its lawful basis, it will carry out and record a Legitimate Interests Assessment where appropriate. This will document:

- the legitimate interest being pursued;
- why the processing is necessary for that purpose; and
- the balancing of those interests against the rights, freedoms and reasonable expectations of the individuals concerned, including any safeguards or mitigation measures.

5.5. The outcome of Legitimate Interests Assessments will be recorded and kept under review, particularly if the nature, scope, context or purpose of the processing changes.

5.6. Special Category Data and Criminal Offence Data will only be processed where an appropriate lawful basis applies and an additional condition for processing such data is satisfied. This may include, for example, explicit consent, employment law obligations, substantial public interest conditions, safeguarding, equality monitoring, legal claims, health or disability support, or another condition set out in the Data Protection Act 2018. The relevant condition will be documented and reflected in the applicable privacy notice where required.

5.7. SIRM College may process personal data in connection with its education, regulatory, contractual and governance responsibilities. This may include, where lawful and necessary, processing or sharing personal data in connection with admissions, enrolment, student support, teaching and learning, assessment, academic appeals, complaints, safeguarding, Prevent, equality monitoring, attendance, funding, student loans, immigration compliance, external quality assurance, awarding body requirements, validating partner requirements, regulatory reporting, audit, governance and institutional risk management.

5.8. Staff must not process personal data simply because it is convenient or potentially useful. Personal data must only be processed where there is a clear purpose, an appropriate lawful basis, and the processing is necessary and proportionate.

6. Transparency

6.1. SIRM College will provide clear and accessible information to individuals about how their personal data is used by means of privacy notices and other relevant communications. Privacy notices will be written in plain language, tailored to the relevant audience, and made available at the point personal data is collected or as soon as reasonably practicable afterwards.

6.2. SIRM College will maintain appropriate privacy notices for different categories of individuals and processing activity. These may include, where relevant, applicant and student privacy notices, staff privacy notices, website and cookies notices, CCTV notices, marketing and recruitment privacy information, online learning, virtual learning environment and recorded session privacy information, and privacy information relating to complaints, safeguarding, Prevent, student support or other casework processes..

6.3. Privacy notices will explain, as appropriate, what personal data is collected, why it is collected, the lawful basis for processing, who it may be shared with, how long it will be retained, individuals' rights, and how to contact SIRM College about data protection matters.

6.4. Staff must ensure that individuals are not misled about how their personal data will be used. Where a new processing activity is introduced, or where personal data is to be used for a materially different purpose, the relevant privacy information must be reviewed and updated where required.

7. Purpose limitation

7.1. Personal data will only be collected for specific, explicit and legitimate purposes, and will not be used in a way that is incompatible with those purposes.

7.2. If SIRM wishes to use personal data for a new purpose that is different from, but compatible with, the original purpose, individuals will be informed and any additional legal requirements will be met.

7.3. Where the new purpose is incompatible with the original purpose, fresh consent or another appropriate lawful basis will be obtained before processing.

7.4. Staff must not reuse personal data for a new activity, report, system, project, partnership arrangement, marketing activity, monitoring activity or data sharing arrangement unless the purpose has been considered, the lawful basis has been confirmed, and the relevant privacy information has been reviewed.

8. Data minimisation

8.1. SIRM will only collect and retain the minimum amount of personal data needed to fulfil the stated purposes. Staff must not collect personal data "just in case" it might be useful in future.

8.2. Forms, systems and processes will be designed to avoid collecting unnecessary data. Existing data collections should be reviewed periodically to ensure that all fields and categories remain necessary and proportionate.

8.3. Staff must ensure that reports, spreadsheets, emails, casework notes, assessment records, attendance records, complaints records and other documents only include the personal data that is necessary for the purpose for which the information is being used.

8.4. Where anonymised or aggregated data would be sufficient, staff should use anonymised or aggregated data rather than identifiable personal data.

9. Accuracy

9.1. Personal data must be accurate and, where necessary, kept up to date. SIRM will take reasonable steps to check the accuracy of personal data at the point of collection and at appropriate intervals afterwards.

9.2. Inaccurate or incomplete personal data will be rectified or erased without undue delay once identified, taking into account legal obligations and the context in which the data is used.

9.3. Staff must take particular care where personal data is used for admissions, enrolment, attendance monitoring, student support, assessment, progression, funding, regulatory reporting, immigration compliance, complaints, safeguarding, Prevent, HR, payroll, finance or governance purposes.

9.4. Where staff become aware that personal data may be inaccurate, incomplete, duplicated, outdated or recorded against the wrong individual, they must take appropriate steps to correct or escalate the issue without delay.

10. Storage limitation and data retention

10.1. Personal data must not be kept for longer than is needed for the purposes for which it was collected. When personal data is no longer required, it will be securely destroyed, erased or anonymised, in line with SIRM Data Retention Policy and Retention Schedule.

10.2. SIRM will maintain a Data Retention Schedule setting out standard retention periods for key categories of personal data, including staff, student, applicant, alumni where applicable, governance, complaints, casework, assessment, finance, supplier and partner records. Retention periods will take into account legal, regulatory, contractual, professional, awarding body, validating partner and sector-specific requirements, including the requirements of the Office for Students where applicable.

10.3. In relation to students' assessed work and associated assessment records, including examination scripts, coursework submissions, feedback, marks, moderation documentation and assessment or exam board records, SIRM College will retain such information for long enough to:

10.3.1. complete internal and external quality assurance processes;
10.3.2. meet awarding body and validating partner requirements;
10.3.3. enable the handling of academic appeals, complaints, academic misconduct cases, student support cases, safeguarding or Prevent cases, harassment and sexual misconduct cases, and other matters arising under institutional student-related procedures; and
10.3.4. demonstrate compliance with relevant Office for Students ongoing conditions of registration, particularly those relating to academic standards, assessment, awards and the quality of courses.

10.4. To meet these requirements, SIRM will retain a proportionate sample of students' assessed work and related assessment records for a minimum period of five years after the student has completed or left the course, unless a longer or shorter period is specified in SIRM Data Retention Schedule, awarding body requirements, validating partner requirements, legal obligations, regulatory obligations or another documented institutional requirement.

10.5. At the end of the applicable retention period, students' assessed work and related assessment records will be securely destroyed, erased or anonymised so that individual students can no longer be identified, unless a longer retention period is properly justified and documented, for example because of ongoing legal, regulatory, complaint, appeal, safeguarding, Prevent, misconduct or quality assurance proceedings.

10.6. Staff must not retain personal data in local files, personal drives, email accounts, downloads folders, portable devices, paper files or informal spreadsheets outside approved SIRM systems unless there is a clear business need and appropriate security arrangements are in place.

10.7. Where personal data is retained beyond the usual retention period, the reason must be documented and reviewed periodically.

11. Security, integrity and confidentiality

11.1. SIRM will implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

11.2. Security measures will be proportionate to the nature, sensitivity and volume of the personal data and may include, for example, access controls, multi-factor authentication, encryption, pseudonymisation, secure configurations, physical security, back-up and recovery arrangements, monitoring, audit logging, staff training and regular testing.

11.3. Staff must follow all information security policies and procedures, use only approved systems and storage locations, keep passwords and authentication methods secure, and take care when sharing or transmitting personal data.

11.4. Personal data must not be stored in personal email accounts, personal cloud storage, unauthorised devices, informal spreadsheets, removable media or unapproved systems unless this has been authorised and appropriate security measures are in place.

11.5. Access to personal data must be limited to those who need it for a legitimate SIRM purpose. Access permissions must be reviewed periodically and updated promptly when staff join, leave or change roles.

11.6. Staff must take particular care when using email, shared links, shared drives, Microsoft 365, SharePoint, Teams, the virtual learning environment, student record systems, assessment systems, HR systems and any other platform used to store or share personal data.

11.7. Data security encompasses:

11.7.1. confidentiality, ensuring that only authorised individuals have access to the data;
11.7.2. integrity, ensuring that data is accurate, complete and reliable for its intended use; and
11.7.3. availability, ensuring that authorised users can access the data when required for legitimate purposes

11.8. Physical records containing personal data must be stored securely, protected from unauthorised access, and disposed of securely when no longer required. Staff must take particular care when printing, scanning, transporting or working with personal data across campuses or away from SIRM premises.

11.9. Failure to comply with data security requirements may result in disciplinary action and, where appropriate, may also have legal, contractual, regulatory or professional consequences.

12. International transfers

12.1. Personal data must not be transferred outside the UK unless appropriate safeguards are in place and the transfer complies with data protection law.

12.2. A transfer may include sending personal data to another country, allowing personal data to be accessed from another country, storing personal data on systems hosted outside the UK, or using suppliers, agents, consultants or cloud services that process personal data outside the UK.

12.3. SIRM will only transfer personal data outside the UK where there is a lawful basis for the processing and an appropriate transfer mechanism or safeguard is in place. This may include adequacy regulations, the International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another lawful mechanism recognised under UK data protection law.

12.4. Staff must not store, send, access or transfer personal data using services, systems, devices or suppliers that involve international transfers unless those arrangements have been assessed and approved in line with SIRM information governance, procurement and data protection processes.

12.5. Particular care must be taken where personal data is shared with or accessed by overseas agents, international recruitment partners, overseas consultants, cloud service providers, IT support providers or other third parties outside the UK.

12.6. Where an international transfer is proposed, staff must seek advice from the Data Protection Officer or nominated operational lead before the transfer takes place.

13. Data subject rights and requests

13.1. Individuals have a range of rights in relation to their personal data. These rights apply in specific circumstances and include:

- the right to be informed about how their data is used
- the right of access to their personal data
- the right to have inaccurate data corrected
- the right to have personal data erased in certain situations
- the right to restrict processing in certain situations
- the right to data portability, enabling them to obtain and reuse their data in a structured, commonly used and machine-readable format
- the right to object to certain types of processing, including direct marketing or processing based on legitimate interests
- rights related to automated decision-making and profiling

- the right to withdraw consent where consent is the lawful basis for processing
- the right to be notified of certain personal data breaches that are likely to result in a high risk to their rights and freedoms
- the right to lodge a complaint with the Information Commissioner's Office or another supervisory authority.

13.2. Requests from individuals to exercise any of these rights, including requests for access to personal data, must be handled promptly and in line with legal timescales and internal procedures.

13.3. A Subject Access Request must be responded to without undue delay and within one month, unless an extension is permitted under data protection law. Where clarification or identity verification is reasonably required, this must be requested promptly and recorded.

13.4. A request does not need to use the words "Subject Access Request" and may be made verbally or in writing. Staff must treat any request for access to personal data, or any request relating to data protection rights, as potentially valid and must escalate it without delay.

13.5. Staff who receive a written or verbal request relating to personal data must forward it without delay to their line manager, the Compliance team, the nominated operational lead or the Data Protection Officer. Staff must not respond substantively unless authorised to do so.

13.6. Subject Access Requests and other data subject rights requests will be coordinated by the Compliance team or another nominated operational lead, with oversight and advice from the Data Protection Officer.

13.7. The Data Protection Officer must be involved where a request is complex, sensitive, contested, high-risk, involves third-party data, requires exemptions or redactions, relates to complaints, appeals, disciplinary, safeguarding, Prevent, harassment, misconduct, HR or legal matters, or may give rise to regulatory, legal or reputational risk.

13.8. SIRM will keep appropriate records of data subject rights requests, including the date received, scope of the request, identity checks, clarification sought, searches undertaken, exemptions applied, redactions made, response date, outcome and any learning or follow-up actions.

13.9. Please see Annex 1: Subject Access Request Protocol at the end of this policy for the procedure that must be followed in the event of a Subject Access Request or similar request.

14. Automated processing and automated decision-making

14.1. Where SIRM uses profiling or automated decision-making that produces legal effects concerning an individual, or similarly significantly affects them, additional safeguards will be applied in line with data protection law.

14.2. Automated decision-making may include decisions made without meaningful human involvement. Profiling may include the automated use of personal data to evaluate, analyse or predict aspects of an individual's performance, behaviour, preferences, attendance, engagement, risk, support needs or other characteristics.

14.3. Any proposals for new or changed profiling or automated decision-making activities must be referred to the Data Protection Officer before implementation and may require a Data Protection Impact Assessment.

14.4. Particular care must be taken where SIRM proposes to use artificial intelligence tools, learner analytics, automated risk indicators, automated attendance or engagement monitoring, automated admissions tools, automated marketing tools, or any system that may influence decisions about students, applicants, staff or other individuals.

14.5. Individuals affected by qualifying automated decision-making will normally be given meaningful information about the logic involved, the significance and envisaged consequences of the processing, and the opportunity to obtain human intervention, express their point of view and, where appropriate, contest the decision.

14.6. SIRM will not make solely automated decisions that have legal or similarly significant effects on individuals unless this is permitted under data protection law and appropriate safeguards are in place.

15. Direct marketing

15.1. SIRM will comply with data protection and e-privacy requirements when carrying out direct marketing activities, including email, SMS, telephone, postal marketing, online advertising, events, open days, applicant communications, alumni communications and other recruitment or promotional activity.

15.2. Appropriate consent or another lawful basis will be used for marketing, and individuals' marketing preferences will be respected and recorded. Opt-out mechanisms must be simple, clear and effective.

15.3. Staff must follow SIRM direct marketing, admissions, recruitment and communications procedures and must not use personal data for unsolicited marketing outside these arrangements.

15.4. Particular care must be taken where marketing activity involves prospective students, applicants, alumni, schools, employers, agents, partners or third-party platforms.

15.5. Personal data collected for admissions, student administration, support, assessment, complaints, safeguarding, Prevent, HR or other institutional purposes must not be reused for marketing unless the proposed use is lawful, transparent, compatible with the original purpose, and individuals' preferences have been checked.

15.6. SIRM will ensure that marketing lists, consent records, opt-outs and suppression lists are maintained accurately and reviewed periodically.

16. Personal data breaches and notification

16.1. A personal data breach may occur through, for example, loss or theft of devices or documents, misdirected emails, unauthorised access to systems, incorrect sharing permissions, accidental disclosure, alteration or deletion of data, cyber incidents, malware, phishing, loss of paper records, technical failures, or any other incident that compromises the security, confidentiality, integrity or availability of personal data.

16.2. All suspected or actual personal data breaches must be reported immediately to a line manager, the Compliance team, the nominated operational lead or the Data Protection Officer using SIRM incident reporting processes.

16.3. Staff must not delay reporting a suspected breach because they are unsure whether it is serious or whether personal data has definitely been compromised. Suspected breaches must be escalated promptly so that they can be assessed.

16.4. Staff must not attempt to investigate incidents themselves beyond taking immediate steps to contain any obvious risk. Staff must preserve any evidence that may be needed, including emails, files, screenshots, access logs, audit logs, system records, shared links, correspondence and notes of action taken.

16.5. SIRM will assess reported incidents promptly to determine whether a personal data breach has occurred, the likely impact on individuals, the containment action required, whether the incident must be notified to the Information Commissioner's Office, and whether affected individuals must be informed.

16.6. The Data Protection Officer must be involved in the assessment of personal data breaches, particularly where the breach involves special category data, criminal offence data, student casework, safeguarding, Prevent, complaints, assessment records, staff records, large volumes of data, external disclosure, regulatory risk, legal risk or reputational risk.

16.7. Where a notifiable breach is likely to result in a risk to the rights and freedoms of individuals, SIRM will report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it.

16.8. Affected individuals will be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

16.9. SIRM will maintain a personal data breach log, including suspected breaches and near misses. The log will record the nature of the incident, date and time identified, date and time reported, individuals or data affected, containment action, risk assessment, notification decision, outcome, lessons learned and any follow-up actions.

16.10. Serious breaches, repeated incidents, significant near misses or issues indicating control weaknesses will be escalated to the Principal and reported through the relevant governance route for assurance and oversight.

17. Training and awareness

17.1. All new staff will receive basic data protection and information security training as part of their induction.

17.2. Refresher training and targeted guidance will be provided periodically so that staff remain aware of their responsibilities and understand how to handle personal data securely and lawfully in their roles.

17.3. Staff in roles involving higher-risk processing may be required to complete additional or targeted training. This may include staff involved in admissions, registry, student support, safeguarding, Prevent, complaints, academic appeals, assessment, HR, finance, IT, marketing, governance, international recruitment, agent management or partner management.

17.4. SIRM will maintain records of data protection training completion and will monitor completion as part of its compliance and assurance arrangements.

17.5. The Data Protection Officer will provide advice on data protection awareness, training needs and areas where additional guidance may be required. Operational coordination of training records may be undertaken by the Compliance team or another nominated operational lead.

17.6. Failure to complete mandatory training or to follow the requirements of this policy may be treated as a disciplinary issue and may also result in other action where appropriate.

18. Records and documentation

18.1. SIRM will maintain appropriate records of its data processing activities, including Records of Processing Activities, data sharing arrangements, Data Protection Impact Assessments, Legitimate Interests Assessments, retention schedules, processor records, privacy notices, security measures, training records, breach records and Subject Access Request records, as required by UK GDPR and associated guidance.

18.2. Data Protection Impact Assessments will be carried out for processing activities that are likely to result in a high risk to individuals' rights and freedoms, such as large-scale processing of sensitive data, systematic monitoring, new technologies, significant changes to systems, use of artificial intelligence tools, learner analytics, or new data sharing arrangements involving sensitive or high-risk personal data.

18.3. The outcomes of Data Protection Impact Assessments, including any mitigating measures, will be documented, monitored and reviewed where the processing changes or where risks increase.

18.4. Legitimate Interests Assessments will be undertaken and documented where appropriate whenever SIRM relies on legitimate interests as a lawful basis, to ensure that those interests are balanced appropriately against individuals' rights, freedoms and reasonable expectations.

18.5. SIRM will maintain records of third-party processors and relevant data sharing arrangements. These records should identify, where appropriate, the nature of the personal data processed or shared, the purpose of the processing or sharing, the lawful basis, the parties involved, retention requirements, security expectations and any contractual or assurance requirements.

18.6. SIRM will retain appropriate records to demonstrate compliance with this policy, including evidence of advice provided, decisions made, audits undertaken, actions completed, breaches assessed, requests handled, training completed and governance reports submitted.

18.7. These records and assessments will be reviewed and updated when processing activities, associated risks, systems, suppliers, partners, campuses, delivery arrangements, legal requirements or regulatory expectations change.

19. Monitoring and review

19.1. This policy and related procedures will be reviewed annually, and earlier where there are significant changes to law, regulation, ICO guidance, SIRM activities, systems, data processing arrangements, campuses, partnerships, suppliers or governance arrangements.

19.2. This policy may also be reviewed earlier following a serious personal data breach, repeated data protection incidents, a significant Subject Access Request issue, an ICO complaint or enquiry, an audit finding, a material change to the role or reporting line of the Data Protection Officer, or any other matter indicating that the policy or associated procedures may no longer be effective.

19.3. The Data Protection Officer will monitor compliance with this policy and may recommend changes to policies, procedures, training, systems, records, access controls, data sharing arrangements, retention arrangements or other controls where required.

19.4. Periodic data protection assurance reporting will be provided through SIRM's governance arrangements, including the Compliance and Quality Committee for compliance assurance, the Finance, Audit and Risk Committee for risk, audit and information security matters, and the Board of Governors for ultimate oversight. This may include reporting on::

- Subject Access Requests and other rights requests
- personal data breaches, near misses and lessons learned
- Data Protection Impact Assessments
- Legitimate Interests Assessments
- training completion and awareness activity
- data protection audits and action plans
- processor and supplier oversight
- data sharing arrangements
- retention and deletion compliance
- access control and information security issues
- ICO contact, complaints or regulatory matters

Updates to this policy will be approved through SIRM governance processes and communicated to staff and other relevant stakeholders. Significant risks, themes or improvement actions will be escalated through the Compliance and Quality Committee, the Finance, Audit and Risk Committee, the Senior Leadership Team and/or the Board of Governors, depending on the nature and seriousness of the matter..

1. Annex 1: Subject Access Request Procedure

The following protocol must be followed where SIRM College receives a Subject Access Request or any request from an individual to access their personal data.

Receipt and logging

A Subject Access Request may be made verbally or in writing. It does not need to use the words "Subject Access Request" or refer specifically to data protection law.

All staff must treat any request for access to personal data as potentially valid and must forward it immediately to the Compliance team, nominated SAR handler or Data Protection Officer.

The request must be logged with:

- the date received
- the requester's details
- the scope of the request
- the method of receipt
- the allocated handler
- the statutory deadline
- any identity verification or clarification required.

An acknowledgement should normally be sent within 5 working days by the Compliance team, nominated SAR handler or another authorised person. The acknowledgement should explain the normal one-month deadline and request identity verification or clarification where this is reasonably required.

Verify identity and clarify scope

Where necessary, SIRM may request reasonable proof of identity before disclosing personal data. The level of identity verification required should be proportionate to the nature and sensitivity of the information requested.

Where a request is unclear, broad or difficult to action, SIRM may ask the requester to clarify the scope of the request. This may include asking for further information about:

- the date range of the information requested
- the type of records requested
- the relevant department, campus, course, process or system
- the individuals likely to hold relevant information
- whether the request relates to a specific issue, complaint, appeal, case or decision.

Requests for identity verification or clarification must be made promptly and must be recorded on the Subject Access Request log.

Staff must not use clarification requests to delay or obstruct a valid request. Any clarification sought must be reasonable, necessary and proportionate.

Where there is uncertainty about whether clarification is needed, whether the deadline may be affected, or whether the request is complex, advice should be sought from the Data Protection Officer.

Locate and collect information

The Compliance team, nominated SAR handler or other authorised person will identify the areas, systems and staff likely to hold relevant personal data.

Relevant areas may include, where applicable:

- Admissions
- academic departments
- student support
- safeguarding
- Prevent
- complaints and appeals
- misconduct or disciplinary records
- assessment and quality records
- finance
- HR
- IT
- marketing and recruitment
- governance records
- email accounts
- shared drives
- Microsoft 365, SharePoint and Teams
- the virtual learning environment
- student record systems
- paper files and archived records.

Staff asked to search for information must follow the search instructions provided and must return results by the internal deadline set by the SAR handler.

Search results should include all personal data within scope, whether favourable, unfavourable, informal, historic, duplicated or held in emails, notes, attachments, spreadsheets, case records or system records.

Staff must not delete, alter, conceal or withhold information because a Subject Access Request has been received.

Where relevant information may be held by a processor, partner, supplier, awarding body, validating partner, agent or other third party acting on behalf of SIRM the SAR handler must consider whether that information should be requested and included in the response.

A record must be kept of the searches requested, the systems or locations searched, the staff involved, the date searches were completed, and any areas where no relevant information was found.

Review and (where strictly necessary) redact

The SAR handler will review the information collected to identify the requester's personal data and remove information that is outside the scope of the request.

The review should consider whether the information includes:

- duplicate material

- irrelevant material
- personal data relating to third parties
- confidential references
- legally privileged material
- management planning information
- examination scripts or assessment-related information subject to specific rules or exemptions
- information connected to complaints, appeals, safeguarding, Prevent, misconduct, disciplinary, HR or legal matters
- information that may be subject to an exemption under data protection law.

Third-party personal data must be reviewed carefully. It should not normally be disclosed unless the third party has consented, it is reasonable to disclose it without consent, or the information can be appropriately redacted.

Redactions must be applied carefully and consistently. The reason for any redaction or withheld information must be recorded.

The Data Protection Officer should be consulted where the request is complex, sensitive, high-risk, involves third-party data, requires exemptions, or may create legal, regulatory or reputational risk.

Staff must not apply exemptions or withhold information without appropriate advice or authorisation.

Prepare and issue the response

The SAR handler will prepare the response for the requester, ensuring that the response is clear, accurate and limited to the personal data that should properly be disclosed.

The response should include, where applicable:

- a copy of the requester's personal data
- an explanation of the purposes of processing
- the lawful bases for processing
- the categories of personal data concerned
- the recipients or categories of recipients to whom the data has been or may be disclosed
- the applicable retention period or retention criteria
- information about the requester's data protection rights
- information about the right to complain to the Information Commissioner's Office
- information about any exemptions relied upon, where appropriate.

The response should be provided in a secure and accessible format, taking into account the nature and sensitivity of the information and the requester's circumstances.

The response must normally be issued without undue delay and within one month of receipt of the request, unless an extension is permitted under data protection law.

Where a request is complex or numerous, SIRM College may extend the response period by up to a further two months. The requester must be informed within the first month if an extension is being applied and must be told the reason for the extension.

The Data Protection Officer should review or approve the response before issue where the request is complex, sensitive, high-risk, involves extensive redactions, relies on exemptions, or may create legal, regulatory or reputational risk.

A copy of the final response and disclosed information must be retained in accordance with SIRM retention requirements.

Record-keeping and follow-up

The SAR handler will update the Subject Access Request log once the response has been issued.

The log should record:

- the date the request was received
- the identity checks or clarification requested
- the scope of the request
- the searches undertaken
- the departments, systems and records searched
- the date the response was issued
- whether any extension was applied
- whether any information was withheld or redacted
- the reason for any exemptions or redactions
- any complaint, challenge or follow-up from the requester
- any learning points or improvement actions.

The SAR handler will ensure that any learning points or process improvements are recorded and shared with the Data Protection Officer.

Where the SAR identifies weaknesses in record-keeping, access controls, retention, email use, case management, privacy information or staff understanding, the Data Protection Officer may recommend further action, training, audit or governance reporting.

Repeated issues, serious concerns or requests indicating wider control weaknesses should be escalated through SIRM governance arrangements.

SAR records must be retained in accordance with SIRM Data Retention Policy and Retention Schedule.