Purpose
SIRM processes information about its staff, applicants, students, alumni and other persons for purposes such as the administration, operate HR & run payroll as well as the effective provision of academic and welfare services. This policy aims to ensure that SIRM complies with General Data Protection Regulations (GDPR) and that personal information is processed and used fairly, stored securely and not disclosed to any unauthorised person.

Scope
This policy applies to all staff of SIRM where they are acting in the course of their duties as its employees and to students, other members of SIRM where they are acting on its behalf or under its instruction. It applies to all personal data acquired, held and used by SIRM, regardless of format (paper or digital) and location (processed on SIRM premises or elsewhere).

Personal Information
Personal information means any information or pieces of information that can directly identify a person such as by name or indirectly via combinations of data including unique ID numbers, address, etc. This can also include email and home addresses, usernames, personal preferences, shopping habits, user-generated content and unique numerical identifiers such as a computer's IP address. Some of the data that we may hold about you may be regarded as 'sensitive personal data'. Examples of such data are health conditions or ethnic origins.

Information Collection Principles
Everyone at SIRM who collect process or use any personal information must ensure that they follow these principles at all times.

Personal Information must:

- be obtained and processed fairly, lawfully and transparently
- be obtained for specified, explicit and legitimate purposes only and not used in any other way without the person's consent
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be kept for longer than it is necessary
- kept, processed and handled in a manner that is safe from unauthorised access, unlawful processing, accidental loss or destruction

Collection of information
SIRM will review on an ongoing basis all categories of personal information that is collected to ensure that there is a legitimate reason to justify its collection and processing. On collection of personal information, SIRM will ensure that consent is freely given and data subjects have access to SIRM's approach to processing, sharing and retaining data.

Processing of information
When processing data SIRM will ensure one of the below lawful bases for processing as set out in Article 6 of the GDPR applies:

- Consent - the person has given clear consent for their personal information to be processed for a specific purpose.
- Contract – the processing is necessary for a contract you have with the person, or because they have asked you to take specific steps before entering into a contract.

- Legal obligation – the processing is necessary for SIRM to comply with the law.
- Vital interests – the processing is necessary to protect someone's life.
- Public task – the processing is necessary for SIRM to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- Legitimate interests - the processing is necessary for SIRM's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

SIRM will ensure that it gives staff appropriate instructions regarding how they are to handle personal information on SIRM's behalf. This will include:

- if they can share the information and how they do this securely
- processing in line with appropriate consent
- how they store information securely
- how they can respond to questions, concerns or incidents

Data will only be processed in line with its original purpose for collection unless there is a legal basis or further consent is gained. All data subjects will be able to access the information that SIRM holds on them to ensure its accuracy, to correct their data or to withdraw consent at any time (where consent has been asked for).

Sharing Personal Information with Partners

Personal information will only be shared with third party organisations where there is a legitimate purpose; data subjects have been informed with the relevant level of consent has been sought. When sharing personal and/or special category data with other organisations SIRM will ensure that this is done by secure means ensuring it can only be accessed by the intended recipient. For organisations that SIRM share personal data SIRM will seek assurance that there approach to processing personal and/or special category data is compliant with GDPR.

Retention of Data

SIRM will ensure that data will only be retained for a period that is necessary for business or legal purposes.

Rights of Data Subjects

SIRM is committed to ensuring all data subjects are able to exercise their rights under the regulation and below details how SIRM upholds these rights:

- Right to be informed – SIRM Privacy Statement clearly sets out SIRM approach to how and why we process data.
- Right of access - all requests to access personal and/or special category data must be made in writing to the Data Protection Officer. It is called a Subject Access Request. These will be responded to within one calendar month.
- Right to rectification – data subjects are entitled to ask SIRM to correct, complete or update any personal information which SIRM holds. All requests in the first instance should be directed to the relevant department.
- Right to erasure – data subjects may ask SIRM to delete or remove personal information which is no longer necessary in relation to the purpose for which it was originally collected or processed or have objected to it being processed and the continued use of that data cannot be justified. However, SIRM may have a legitimate interest or a legal or contractual obligation to do so. In this instance, SIRM processing will be limited to what is necessary to fulfil these interests or obligations. All requests to

remove personal data must be made in writing to the Data Protection Officer. These will be responded to within one calendar month.

- Right to restrict processing – this may arise because data subjects wish to establish the accuracy of the information or establish the reason for processing it or if data subjects object to the processing. All requests in the first instance should be directed to the relevant department.
- Right to data portability – data subjects may ask for the transfer of their personal information to another party when the processing is based on consent and executed by automated methods. This does not apply to any data processing that SIRM may carry out. All requests must be made in writing to the Data Protection Officer. These will be responded to within one calendar month.
- Right to object – in SIRM's data collection processes and communications with data subjects, SIRM will ensure it is clear how to exercise the right to object. All requests in the first instance should be directed to the relevant department.

Roles and Responsibilities

Staff

All staff at SIRM are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Any personal data is not disclosed to any unauthorised person (orally, in writing or electronically)

Any unauthorised disclosure of personal information will attract disciplinary action against the staff.

When not in use, personal information should be:

- Kept in a locked filing cabinet; or
- If it is in electronic format, either be password protected or kept only on a storage device which is encrypted and kept securely.

In respect of their own personal data, staff have the responsibility to:

- ensure that any information they provide to SIRM in connection with their employment is accurate and up to date; and
- inform SIRM of any changes to information that they have provided.

In respect of all other personal data that staff hold, process or have access to in connection with their employment they are responsible for ensuring that they comply with these procedures.

Students

Students must ensure that all personal data provided to SIRM is accurate and up to date. Students must ensure that any changes in personal details are notified to the appropriate person.

Data Protection Officer

SIRM as a body is the data controller under the Regulation, and Senior Leadership Team is therefore ultimately responsible for implementation. However, the designated Data Protection Officer is appointed to deal with day-to-day matters to ensure processes are robust and in line with the legislative requirements.

Enforcements and Breaches

Any loss of data must be reported to the Data Protection Officer for an assessment of the risks associated with the breach.

In addition, if special or personal data about a student or member of staff is either inadvertently released or used inappropriately, the Data Protection Officer is to be informed as soon as the breach is discovered so that appropriate action can be taken.

The Data Protection Officer is responsible for:

- informing appropriate people and organisations that the breach has occurred;
- notifying serious breaches (based on current ICO guidance);
- implementing a recovery plan, including damage limitation; and
- reviewing and updating information security;

Types of information

We collect and use the following types personal data:

- Staff:
    - recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;

- Name
- Address
- Email and other contact details
- Date of birth
- Job history (including information relating to placements through us)
- Educational history, qualifications& skills
- Visa and other rights to work or identity information
- Passport number
- National insurance number
- Next of kin and family details
- Contact details of referees
- Personal information relating to hobbies, interests and pastimes
- The information contained in references
- Other sensitive personal information such as health or learning records
- Your marketing preferences
- Proof of your right to live in the UK/EU (passport, visa, resident permit)
- Our records on your attendance and any welfare or behaviour issues

We collect personal information from the following:

These are instances when you have directly given us personal data:

- Completed enquiry forms
- Completed registration forms including next of kin details in case of emergencies
- Competed application forms
- CV
- Copies of certificates of qualifications/training previously achieved
- Other documentation such as learning styles questionnaires and equal opportunity forms
- Incoming emails
- Telephone and video conference calls
- During interviews (this includes notes taken during interviews)

- Examination/assessment bookings

There will also be occasions when we collect data from other means such as:

- Documents freely available to the public (i.e. electoral roll, third party websites)
- Cookies used to track visitor interactions on our website
- Other third parties, such as trusted partners

For tutors/trainers, we will also ask for referee information, references and bank information for payment of fees.

When we first obtain personal information from you, or when you undertake one of our services we will ask you to tell us if you want to receive information from us about other services, events or other matters. You have the right to indicate that you do not want to hear from us. If you choose to receive notifications from us you will be asked about your preferred communication method (telephone, email, post).

On occasions, we may obtain your personal data from a third party such as an educational agent/representative or UCAS during our student recruitment campaigns. In this instance, UCAS or the agent/representative should have informed you that your information may be shared with training providers such as SIRM and you will have consented to this. We will only hold this information on the sole basis that you may be interested in our training courses and programmes.

What we do with the information

In order to answer your enquiries about training and education, to provide you with training/education and to enrol you on courses we need to obtain certain information from you so that we can process your enquiry, application, enrolment and assessment or examination. We will only process the information that you give us to provide you with this service.

We collect personal data for the following purposes:

- To help us to identify you when you contact us
- To help us to advise you with your enquiries
- To assist with the provision of information about any of our past, current or future services
- To enable us to carry out marketing analysis, create learner/enquirer profiles and conduct research
- To carry out an assessment of your suitability for a specific training programme
- To provide information to an awarding body or a delivery or funding partner of ours
- To provide information to a regulatory authority or a statutory body
- To enable us to improve the functionality and design of our website
- To allow us to contact you about our services unless you have stated that you do not wish to be contacted by us
- To help us to identify and prevent loss or fraud
- To ensure that we can conduct equal opportunities monitoring
- To undertake auditing or compliance activities to fulfill contractual obligations that we may have with a trusted partner such as the ESFA or another training provider

Please note:

- We will not keep personal data for longer than is necessary to fulfil the above purposes which we collected it for i.e. the provision of our services
- Our standard data retention period is 6 years from the last date on which we were in contact with you, following this your personal data will be deleted
- We may monitor and record communications such as telephone conversations and emails for quality assurance and compliance checks
- We will not sell your personal information to third parties for the purpose of direct marketing
- We are not responsible for the privacy policies of any third party websites that may be linked to our website
- We are not responsible for any marketing messages which you may receive from third parties who have accessed your IP address via our website
- We can store your personal data on a suppression list so that we can ensure we do not contact you again if you ask us to stop sending you marketing communications, this is a legal obligation

Disclosure of information

Under legal obligations, we may be required to disclose your personal information to the Home Office or any interested government agency and with ESFA and for the Individualised Learner Record (ILR). Reference: https://www.gov.uk/government/collections/individualised-learner-record-ilr

When required to do so in connection with any legal proceedings including prospective legal proceedings we may disclose your personal data to exercise our legal rights.

If SIRM and its assets are acquired by a third party then all the personal data held by us about our students and stakeholders will become a transferred asset.

Sometimes we enter into trusted partnerships with other training providers such as further education colleges and universities to deliver training and in these instances, we would only disclose information which is deemed to be necessary for funding, training and contractual purposes.

The internet and cookies

Communications on the internet through emails, web chats and webmails are not secure unless they have been encrypted. These messages or conversations can be hacked and we cannot accept any responsibility for any unauthorized access or loss of personal data that is beyond our control. As the internet is not a completely secure medium we cannot guarantee the absolute security of personal information.

We use Google Analytics as a marketing tool to track and assess the user's experience on our website. This tool can give us information such as IP address, geographical location, browser type, referral source, length of visit and number (and timing) of page views for each visitor to our website. This information will not be sufficient to personally identify individuals and will only be used for the purposes of improving our website and marketing. Google does these using cookies to evaluate your use of the website and to compile reports for us based on activity on the site. Google stores the information collected by cookies on servers in the United States and they may transfer this

information to third parties when required by law or where third parties process the information on Google's behalf. Google will not associate your IP address with any other data that it holds. Google is a member of the US Safe Harbor Scheme and this scheme is regarded as providing adequate protection for personal data transmitted from Europe.

Cookies are files made up of pieces of text, including unique identifiers which are sent by web servers to web browsers and then may be sent back to the server each time the browser requests a page from the server. They are used by web servers to identify and track users as they navigate different pages on a website and to identify users who return to visit a website. Cookies can be stored in the cookie directory of a person's computer. There are two kinds of cookie, permanent (persistent) or session. Permanent cookies remain in your system after you have left the website and a random number is stored in your computer to determine how frequently a certain user visits our website. Session cookies expire when leaving a website or when you switch off your computer. Cookies are designed to give us information on which web pages users visit and what their journey around our website is like. This helps us to be better informed about how people use our website so we can improve our website and marketing.

Cookies do not contain any information that personally identifies you, but personal information that we store about you may be linked, by us, to the information stored in and obtained from cookies. If you prefer to not have cookies operating on your device then you can adjust the browser settings to turn off the automatic downloading facility. However, if you block all cookies, it may have a negative impact on the usability of many websites. For instance, you may not be able to use password features on some sites and some navigation paths will stop as cookies are required for third-party integration features.

Security

We take security at SIRM very seriously in all aspects of our operations: physical, organizational and technological. We will do our best to take reasonable precautions to prevent unauthorized access to your personal information and which may result in a loss, misuse or alteration of your data and this is reflected in our policies, procedures and processes. For example, paper copies of information containing personal data will be kept

to a minimum and stored in locked facilities and computers will be protected with passwords. All staff are vetted and trained in their induction on the importance of safeguarding and privacy. We also have procedures in place to deal with any suspected breaches in data security and will inform you and any applicable regulator of such breaches were we are legally required to do so.

Children/young people

Where we recruit and enrol young people between the ages of 16 and 18 we will seek parental consent and inform the parents/guardians of what we will do with the information that we take and store. In addition, all staff are required to undertake a DBS vetting procedure.

Consent

We may process your personal data on the basis that you have consented to us doing so for a specific purpose. For example, this may be that you have given us your contact details so that we can respond to you with information that you have requested. In some instances, you may have given

us your written or verbal consent to the use of your information for specific reasons, such as entering you for assessments.

When we ask you to enrol on our training programmes we will ask for certain information that will enable us to process your application and start you on the course and that will enable us to meet the requirements of funding obligations. For example, funding for an apprenticeship course requires that apprentices have lived in the UK for the last 3 years and are UK or EU residents. In this instance, we would need to have evidence of your residency and citizenship status. If you refuse to give your consent during the recruitment, application and enrolment processes we may not be able to accept you on a course or programme.

You are entitled to withdraw your consent to the processing of your personal data for a specific purpose at any point. However, for legal or contractual reasons we may have to continue to retain your personal information but only for the specific legal or contractual purposes. Withdrawal of consent will not have any effect on the lawfulness of any processing based on consent before its withdrawal.

Your rights

Before accessing and providing any personal information we will ask you to confirm your identity so that no other person is able to receive your personal data.

If you wish to access the information we hold about you or to make another request concerning this data, in line with your rights, please contact us. We may charge a fee to meet our administrative/management costs in providing you with the information that we hold on you.

Contact

We may update this policy from time to time, in line with UK and EU legislation and best practice. We recommend that you visit this page again to keep up to date. If you have any concerns about the data that we may hold on you please contact us by email at info@sirm.ac.uk and explain your concerns.

You have a right to complain to the Information Commissioner's Office (ICO) if you think there is a problem in the way that we are handling your data. Visit this page for further information: https://ico.org.uk/concerns/

Address

The School of Information Risk Management
Ilford Chamber, 4th Floor
11 Chapel Road, Ilford
IG1 2DR, UK
www.sirm.ac.uk
info@sirm.ac.uk
020 7078 7029

Security and C

Confidentiality of Student/Learner Files
The 1998 legislation now extends the same level of protection to paper-based files. The company is registered under the Act and information can be found from the Data Protection Officer.

Personal data – i.e. data by which a living person can be identified - must only be "processed" (obtained or held) in accordance with the Data Protection Act (1998). Personal data may include photographs, attendance records, doctor's appointments, exam results, and remarks about an individual in minutes of meetings or memos or letters and press releases, so beware.

Although the student/learner has a right to see his or her own data, you must not pass on details to any third party (eg friend, parent or employer), without authorisation. Please check before disclosing personal data to anyone. You will be held responsible for the confidentiality of your students'/learners data.

There are now eight "Data Protection Principles" which must be followed. These may affect tutors, assessors or verifiers in the following ways:

Applicants' and Students' Obligations
Applicants and students must ensure that any personal data provided to SIRM is accurate and up to date. They must ensure that any changes of address or other personal details are notified to the Admissions and Administration departments. Enroled students are encouraged to update their own contact details, as required. Students must comply with SIRM's IT Acceptable Use Policy for Students. A breach of these regulations will result in disciplinary action.

Sensitive data
Special conditions apply to the collection and holding of "sensitive" data. In this case you must obtain the specific consent of the student/learner (ideally in writing). You may encounter this when gathering information before arranging work placements, outdoor activities or when taking photographs you intend to use later, perhaps for publicity or publication purposes. "Sensitive Data" has a special definition under the Data Protection Act and covers:

- race or ethnic origin
- political belief religious or other beliefs
- trade union membership (or otherwise)
- sexual life
- physical or mental health or condition (including pregnancy, learning or physical disability)
- actual or alleged criminal records or activities

CCTV
SIRM operates a number of CCTV cameras in order to ensure the security of members of SIRM and its property. Queries regarding the operation of the CCTV system should be directed to the Data Protection Officer. Anyone wishing to access their own personal data on the CCTV system, must complete and return an "Access to Personal Data" form with as much information as possible to enable the data to be located (including, if possible, details of the relevant camera, date and time). CCTV images are only kept for 14 days and are then overwritten. It is therefore important that data subject access requests asking for access to CCTV images are submitted as soon as possible.

Photography and the use of Images

All members of SIRM and visitors to SIRM should be aware that the image of a clearly identifiable person comes within the Act's definition of 'personal data'. The image may appear in (and is not exclusive) to the following formats:

- Photographs
- Videos
- Paper & e-publications
- The internet
- CCTV
- Mobile phones

In order to comply with the Act, explicit consent for any clearly identifiable person will be obtained prior to taking the image and/or before any publication of the image.

All images will be stored securely and used only for their intended purposes.

At SIRM events, every effort will be taken to obtain consent from individuals and groups before a photograph is taken or published, stating the purpose for taking the photograph and its intended use. Images will not be used on the website without prior consent from the person(s) featuring.

Guidance on the use of images and image consent forms are available on VLE.

All photographs and images that are taken by SIRM will be reviewed for long-term preservation in the archive.

Archives

SIRM archive records include:

- Administrative records
- Academic records
- Annual Reports
- Committee files
- Financial records and associated papers
- Legal records
- Minutes
- Operational records
- Personnel records
- Photographs
- Printed material
- Publications
- Student Handbooks

After a member of staff leaves SIRM, his or her personnel file will be transferred to SIRM's archives once it is no longer required for administrative purposes.

After a student has completed their course his or her tutorial records are stored securely for two years in the Student Records Office and then transferred to SIRM Archives.

Security and non-disclosure

You are responsible for the security of any personal data you hold on your students/learners and you are required to take all steps to ensure their data remains secure.

- all paper-based records held on you students/learners must be stored in a secure location. This may be a locked drawer, cupboard or cabinet in a lockable office.
- when using the IT network to store information, don't disclose your password to anyone
- don't leave your IT portable storage devices (such as USBs) containing student data lying around: keep them locked away
- don't include confidential information about students in emails (this includes your intentions or opinions concerning them). Emails can be very easily intercepted.

Further advice may be obtained from the company's Data Protection Officer if you are in doubt about disclosing any personal information.

Right to Access Personal Data

Individuals have the right under the Act to access any personal information that is being held about them by SIRM and to request the correction of such information if it is incorrect. An individual who wishes to exercise his/her right of access is asked to complete SIRM "Access to Personal Data" form available from the Data Protection Officer. Any inaccuracies in the data disclosed in this way should be communicated immediately to the Data Protection Officer who shall take appropriate steps to make the necessary amendments. In accordance with the Act, the College reserves the right to refuse repeated requests where a reasonable period has not elapsed between requests. The College will respond to the request for access to personal data within 30 calendar days (including bank holidays and weekends).