GDPR Policy

1. PURPOSE

SECURE RISK MANAGEMENT LTD is registered with the Information Commissioner and complete details of the SECURE RISK MANAGEMENT LTD current entry on the Data Protection
Register can be found on the notification section of the Information Commissioner website.
Our registration number is 11092318
The register entry provides:

• a fuller explanation of the purposes for which personal information may be used
• details of the types of data subjects about whom personal information may be held
• details of the types of personal information that may be processed
• details of the individuals and organisations that may be recipients of personal information collected by SECURE RISK MANAGEMENT LTD
• Information about transfers of personal information SECURE RISK MANAGEMENT LTD

needs to keep certain information about its employees, clients, voluntary members and other users for administrative purposes. It also needs to process information so that legal obligations to funding bodies and government are complied with. When processing such information, the SECURE RISK MANAGEMENT LTD always comply with the Data Protection Principles, which are set out in the General Data Protection Regulations (GDPR). Anyone processing personal data must comply with the eight enforceable principles of good practice. In summary, these state that personal data shall be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure,
- not transferred to countries without adequate protection as set out in Chapter V
- of the GDPR.

Personal data covers both facts and opinions about the individual. With processing, the definition surrounding the intentions of the **data controller** towards the individual, are far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and
'disclosing'. SECURE RISK MANAGEMENT LTD Staff or others who process or use personal information must ensure that they follow these principles at all times.

2. RESPONSIBILITY

The Director is responsible for ensuring that this policy is applied within the association. The Management Rep is responsible for maintenance, regular review and the updating of this policy.

3. STATUS OF THE POLICY

This document sets out the SECURE RISK MANAGEMENT LTD'S policy and procedures to meet the requirements of the GDPR. It will be made available to employees and voluntary members and other external agencies (having a legitimate interest) upon request, although it is not a substitute for the full wording of the Act.

4. THE DATA CONTROLLER

The Management Rep is ultimately responsible for Data Protection, but the SECURE RISK MANAGEMENT LTD Director is regarded as the main Data Controller. In practice local Regional staff are designated as local data protection officers to deal with day to day matters and ensure they comply with the GDPR on an ongoing basis. They will often look to Course Managers for support in this.

5. SUBJECT CONSENT

In many cases, SECURE RISK MANAGEMENT LTD can only process personal data with the consent of the individual and if the data is sensitive, express consent must be obtained.

SECURE RISK MANAGEMENT LTD has a duty to ensure that all staff are suitable for the jobs assigned by the clients. We also have a duty of care to all staff, clients and voluntary members and must therefore make sure that employees and those who use SECURE RISK MANAGEMENT LTD facilities do not pose a threat or danger to other users.

Therefore, all prospective staff, clients and voluntary members will be asked to consent to their data being processed when an offer of employment or inclusion in other SECURE RISK MANAGEMENT LTD activities. A refusal to give such consent may result in the offer being withdrawn. Other relevant policies here are the Criminal Disclosure Checks and Child Protection Policies.

6. STAFF RESPONSIBILITIES (INCLUDING SECURITY PERSONS)

This policy will not be incorporated into contracts of employment, but it is a condition of
employment that employees will abide by the rules and policies made by the SECURE RISK MANAGEMENT LTD from time to time. Any failures to follow this policy can therefore result in disciplinary proceedings. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Controller. If raising the issue with the Data Controller does not resolve it the matter should
be raised as a formal grievance.

6.1. Specific Staff Responsibilities

All staff, including temp and staff such as security persons, have a responsibility for:
Checking that any information that they provide to the SECURE RISK MANAGEMENT LTD in connection with their employment is accurate and up to date.

- Informing the SECURE RISK MANAGEMENT LTD of any changes to information, which
- they have provided, i.e. changes of address, bank details, etc.
- Informing the SECURE RISK MANAGEMENT LTD of any errors or changes in staff information. When staff hold or process information about clients, colleagues or other data subjects (for example, clients' course work, references to other academic institutions, or details of personal circumstances), they should comply with the following Data Protection Guidelines.

- Any personal data, which they hold, is kept securely, for example:

    - Kept in a locked filling cabinet; or:
    - In a locker drawer.
    - If it is computerised, be password protected; or
    - Kept only on disc, which itself is kept securely

- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Any unauthorised disclosure will be investigated as a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member, as unauthorised disclosure can be a criminal offence.

6.2 Staff Use of Personal Data Off-Site, On Home Computers or at Remote Sites

Employees processing personal data off-site should ensure they take reasonable precautions to prevent the data from being accessed, disclosed or destroyed as a result of any act or omission on their part. They should notify the Data Controller immediately in the event of any loss or theft.

7. EMPLOYEE OBLIGATIONS

Clients must ensure that all data provided to the SECURE RISK MANAGEMENT LTD Is accurate and up to date. They must ensure that changes are notified to Regional office staff as appropriate.

7.1. Client Personal Information – The Purposes for which it is Used

Information that we collect, including information that clients give us at the time of agreement, is added to a record. The SECURE RISK MANAGEMENT LTD holds general information about clients, such as name, addresses, telephone numbers and site details.

Information is used in the following ways:

• To provide services to clients. This includes sending information about current and future plans.

• To undertake research in order to help us plan and improve our services. We may contact clients ourselves.

• To provide information about clients to other bodies in accordance with statutory and government requirements.

• To provide information about clients to other bodies in order to provide accreditation and for audit purposes.

• To produce statistical information for publication and to help us plan and improve our services.

Contact details will not be made available, unless individuals have indicated their consent to be contacted as part of an audit of SECURE RISK MANAGEMENT LTD services. Names will not be used or included in its statistical analysis and precautions are taken to minimise the risk that individuals will be able to be identified from the data.

8. ACCURACY OF DATA

Updating is required only "where necessary" on the basis that, provided the SECURE RISK MANAGEMENT LTD has taken reasonable steps to ensure accuracy (e.g. taking up references), data held is presumed accurate at the time it was collated. All employees and voluntary members should be made aware of the importance of providing the SECURE RISK MANAGEMENT LTD with notice of any change in personal circumstances.

9. THIRD PARTIES

Any data which the SECURE RISK MANAGEMENT LTD Receives and processes in relation to third parties, such as visitors, suppliers, former clients and voluntary members, employers, enquirers and other individuals on mailing lists etc. will be obtained lawfully and fairly and dealt with in accordance with the principles and conditions of the GDPR.

Employees should obtain explicit consent from third party data subjects to process such personal data for the purposes expressed and should ensure that there is a mechanism for data subjects to gain access to data about themselves, to prevent the processing of such data for the purposes of direct marketing and to object to the disclosure of such data.

10. SECURITY MEASURES

This policy is designed to fulfil security person requirements and to prevent unauthorised disclosure of/or access to personal data. The following security measures are therefore be used in respect of the processing of any personal data.

Access to personal data on staff, clients and voluntary members is restricted to those members of staff who have a legitimate need to access such data in accordance with the SECURE RISK MANAGEMENT LTD'S notification to the Information Commissioner.

Members of staff authorised to access personal data, will be allowed to do so, only in so far as they have a legitimate need and only for the purposes recorded in the notification.

All persons processing data and individuals requesting access to personal data in accordance with this policy must have familiarised themselves with this policy.

All data will be stored in such a way that access is only permitted by authorised staff, including storage in filing cabinets, computers and other storage systems. Any act or omission which leads to unauthorised access or disclosure could lead to disciplinary action.
Personal data should be transferred under conditions of security commensurate with the anticipated risks and appropriate to the type of data held.

Personal data held electronically should be appropriately backed up and stored securely to avoid incurring liability to individuals who may suffer damage or distress as a result of the loss or destruction of their personal data.

Any disposal of personal data will be conducted in a secure way, normally by shredding. All computer equipment or media to be sold or scrapped must have had all personal data completely destroyed, by re-formatting, overwriting or degaussing (a method of erasing data held on magnetic media).

10.1. Retention of Data

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including the purposes of satisfying any legal, accounting, or reporting requirements.

10.2. Transfer of Data outside the UK

SECURE RISK MANAGEMENT LTD does not transfer personal data outside the UK without the express consent of the data subject.

11. Your rights

Under the GDPR you have a number of important rights free of charge. Under certain circumstances, you have the right to:

• Request access to your personal information and to certain other supplementary information that this Privacy Policy is already designed to address.
• Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
• Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing.
• Object to processing of your personal information where we are processing your personal information for direct marketing purposes.
• Object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you.
• Object in certain other situations to our continued processing of your personal information.
• Request the transfer of your personal information to another party.
• For further information on each of those rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights under the General Data Protection Regulation which is accessible via:
https://ico.org.uk/for-organisations/guide-to-the-general-datarotectionregulation-gdpr/individual-rights/.

Signed:  **Position:** Managing Director **Date**: 1st December 2024