Reference	RSG 007
Version	4
Issue Date	29/03/2024
Approved	MD

Data Protection Policy

1. PURPOSE

This policy applies to Region Security Guarding Ltd in England. Region Security Guarding Ltd Is registered with the Information Commissioner and complete details of the Region Security Guarding Ltd current entry on the Data Protection Register can be found on the notification section of the Information Commissioners web site. www.dataprotection.gov.uk. Our registration number is ZA280804.

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 Region Security Guarding Ltd
• information about transfers of personal information Region Security Guarding Ltd Needs to keep certain information about its employees, 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 Region Security Guarding Ltd Must comply with the Data Protection Principles, which are set out in the Data Protection Act 2018.

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.

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'. Region Security Guarding Ltd Staff or others who process or use personal information must ensure that they always follow these principles.

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 Region Security Guarding Ltd.'s policy and procedures to meet the requirements of the Data Protection Act 2018. 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 Rep is ultimately responsible for Data Protection, but the Region Security Guarding Ltd Director of Resources 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 Data Protection Act on an ongoing basis.

5. SUBJECT CONSENT

In many cases, Region Security Guarding Ltd can only process personal data with the consent of the individual and if the data is sensitive, express consent must be obtained. Agreement to the Region Security Guarding Ltd Processing some specified categories of personal data is a condition of acceptance of a membership of the Association being recognised, and a condition of employment for staff. For example, this includes information about previous criminal convictions, in accordance with the Rehabilitation of Offenders Act 1974. Some jobs or courses or other Region Security Guarding Ltd Activities, will bring staff, and voluntary members into contact with children, including young people between the ages of 16 and 18 or vulnerable adults. The Region Security Guarding Ltd has a duty to ensure that all staff are suitable for the job Activity they are involved. We also have a duty of care to all staff members and must therefore make sure that employees and those who use Region Security Guarding Ltd Facilities do not pose a threat or danger to other users. Therefore, all prospective staff members will be asked to consent to their data being processed when an offer of employment is given. A refusal to give such consent may result in the offer being withdrawn. Other relevant policies here are the Criminal Disclosure Checks.

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 Region Security Guarding 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 Region Security Guarding Ltd in connection with their employment is accurate and up to date.
• Informing the Region Security Guarding Ltd Of any changes to information, which they have provided, i.e. changes of address, bank details, etc.
• Informing the Region Security Guarding Ltd Of any errors or changes in staff information.

When staff hold or process information about colleagues or other data subjects they should comply with the following Data Protection Guidelines.

All staff are responsible for ensuring that:

• Any personal data, which they hold, is kept securely, for example:
o kept in a locked filing cabinet; or
o in a locked drawer;

o if it is computerised, be password protected; or
o kept only on disk, which is itself 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.

9. ACCURACY OF DATA
Updating is required only "where necessary" on the basis that, provided the Region Security Guarding 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 should be made aware of the importance of providing the Region Security Guarding Ltd With notice of any change in personal circumstances.
Where Individual Student Records (ISRs) are kept employees will be entitled to correct any details although in some cases the Region Security Guarding Ltd May require documentary evidence before effecting the correction.

10. THIRD PARTIES
Any personal data which the Region Security Guarding Ltd Receives and processes in relation to third parties, such as visitors, suppliers, former employees and 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 Act. 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.

11. 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 will therefore be required in respect of the processing of any personal data. Access to personal data on staff is restricted to those members of staff who have a legitimate need to access such data in accordance with the Region Security Guarding 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 personal 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).

11.1. Retention of Data
The Region Security Guarding Ltd Will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements.

11.2. Transfer of Data Outside the UK
Region Security Guarding Ltd Does not transfer personal data outside the UK without the express consent of the data subject.

12. USE OF PERSONAL DATA IN RESEARCH
The 2018 act provides certain exemptions for 'research purposes' including statistical or historical purposes. Provided that the purpose of research processing is not measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject.

13. OTHER POLICIES
GDPR Criteria has been reviewed in the GDPR manual contained within this system (GDPR 01) approved by MD

Signed: Z.ISLAM

Date: 29.03.2024

Review Date: 29.03.2025