Reference	RSG 007
Version	4
Issue Date	29/03/2023
Approved	MD

REGION SECURITY GUARDING

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.

• 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