2024

SSIG

SPECIALITY SECURITY INVESTIGATION GROUP

SECURE DOCUMENTS POLICY

SSIG

SPECIALITY SECURITY INVESTIGATION GROUP

SECURE DOCUMENTS POLICY

Table of Contents

Statement of Policy

Speciality Security Investigation Group Limited trading as SSIG-UK Training Division (the Training Centre, we or our) is committed to the highest standards of information security and treats document security and data confidentiality extremely seriously.

This policy and the rules contained in it apply to all staff of Speciality Security Investigation Group Limited trading as SSIG-UK Training Division, irrespective of seniority, tenure and working hours, including all employees, directors and officers, trainers and contractors, temporary and agency workers, learner and fixed-term staff (Staff or Learner).

All Staff of Speciality Security Investigation Group Limited trading as SSIG-UK Training Division must familiarise themselves with this policy and comply with its terms.

Purpose of Policy

In relation to personal data, under the UK General Data Protection Regulation (the UK GDPR), the Employer must:

a) Ensure the security of personal data, including protection against any unlawful or unauthorised data processing and accidental loss, damage or destruction, by utilising appropriate technical or organisational measures;

b) Demonstrate the consideration and integration of data compliance measures into the Training Centre's data processing activities, by implementing appropriate technical or organisational measures; and

c) Be able to demonstrate the use and implementation of such appropriate technical or organisational measures.

The purpose of this policy is to:

a) Protect against any potential breaches of confidentiality;

b) Protect the Training Centre's informational assets and IT systems and facilities against any loss, damage or misuse;

c) Supplement the Training Centre's Data Protection and Security Policy in ensuring that all Staff are aware of and comply with UK laws and the Training Centre's policies and procedures on the processing of personal data; and

d) Raise awareness of and clarify the responsibilities and duties of Staff in respect of information security, data security and confidentiality.

e) This is a statement of policy only and does not form part of learners use of service agreement. The Training Centre may amend this policy at any time, in our absolute discretion, and we will do so in accordance with our data protection and other obligations. A new copy of the policy will be circulated whenever it is changed.

For the purposes of this policy:

Business Information means any of the Training Centre's business-related information other than personal data about customers, clients, suppliers and other business contacts;

Confidential Information means any documentation or other confidential information (belonging to the learner or third parties) processed by the Training Centre;

Personal Data means any information or documentation provided to the Training Centre by a learner, who can then be identified as an individual from that information, either directly or indirectly; and

Sensitive Personal Data means information documented about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), health, sex life, sexual orientation, genetic information or biometric information (where this is used to identify an individual).

Roles and Responsibilities

All Staff have a responsibility for information security. The Employer's Data Protection Officer (Clark Edwards) has overall responsibility for this policy. Specifically, they must:

a) Implement and maintain this policy;

b) Monitor potential and actual security breaches;

c) Ensure Staff are aware of their responsibilities in relation to information security and confidentiality; and

d) Ensure compliance with the UK GDPR and all other relevant legislation and guidance.

Scope of this Policy

This policy covers all written, verbal and digital information held, used or transmitted by or on behalf of the Training Centre irrespective of media. This includes, but is not limited to:

a) Paper records;

b) Hand-held devices;

c) Telephones;

d) Information stored on computer systems; and

e) Information passed on verbally.

f) The information covered by this policy may include:

g) Personal Data relating to learners and staff;

h) Other Business Information; and

i) Confidential Information.

This policy supplements the Employer's Data Protection and Security Policy and other policies relating to data protection, internet, email and communications, and document retention, including the Employer's:

- Employee Privacy Notice.
- Data Retention Policy.
- Communications and Use of Equipment Policy.

The content of these policies must be considered and taken into account alongside this policy.

General Principles

All information must be:

- Treated as commercially valuable; and
- Protected from loss, theft, misuse or inappropriate access or disclosure.

Through the use of appropriate technical and organisational measures all Personal Data, including Sensitive Personal Data, must be protected against: unauthorised and/or unlawful processing; and accidental loss, destruction or damage.

All staff should discuss what security measures (including technical and organisational measures) are appropriate and which exist to protect any information accessed by Staff in the course of being held and in transit to authorised third parties.

Any information, apart from Learner Personal Data, is owned by the Training Centre and not by an individual or team.

Any information must only be used in connection with processing of services provided to learners that is being undertaken for the Training Centre. It must not be used for any other personal or commercial purposes.

Any Personal Data must only be processed for the specified, explicit and legitimate purpose of processing learners training.

Information Management

Any Personal Data must be processed in accordance with:

a) The data protection principles;

b) The Training Centre's policies on data protection generally (including the Data Protection and Security Policy); and

c) The Training Centre's other relevant policies.

d) All Personal Data collected, used and stored must be:

e) Adequate, relevant and limited to what is necessary for the relevant training; and

f) Kept accurate and up to date.

The Training Centre will take appropriate technical and organisational measures to ensure that Personal Data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage. These measures include:

Follow Highfield E-learning Criteria

- Dual-factor authentication.
- The use of strong passwords.
- Password protection on any documents containing Sensitive Personal Data.
- Will not store physical copies of test papers and related documentation

Reduce physical documented data, using only E-assessments through Highfield E-Learning and utilising Highfields portal (www.HighfieldsWorks.com), in accordance with Highfields E-learning criteria. Any Personal Data and Confidential Information must not be kept any longer than is necessary and will be stored and destroyed in accordance with our Data Retention Policy.

Access to Offices and Information

All office doors, office keys and access codes must, at all times, be kept secure. Office keys and access codes must at no time be given to or communicated to any third parties.

All documents containing and any equipment displaying Confidential Information should be placed and positioned so that anyone passing by cannot see them (e.g. through office windows or glass doors).

Any visitors must:

- Sign it at reception;
- Be accompanied by staff at all times; and
- Not be left alone in areas or situations where they may have access to Confidential Information.

Meetings with visitors must, where possible, take place in meeting rooms. If a visitor meeting takes place outside a meeting room, in an office or other room containing Employer information, steps must be taken to ensure no Confidential Information is visible and accessible to the visitors.

All paper documents, backup systems and E-Learning software containing Confidential Information must be secured: whenever desks are unoccupied; and at the end of the working day.

Computers and IT

Where available on our systems, password protection and encryption must be used to maintain confidentiality.

All computers and other electronic devices must be password protected. Such passwords must be changed regularly and must not be recorded anywhere (e.g. written down) or made available to others. To minimise the risk of accidental loss or disclosure, all computers and other electronic devices must be locked when not in use, including when left unattended at a desk.

All data held electronically must be securely backed up as soon as possible in accordance with the Training Centre's internal backup procedure.

Staff must:

- Ensure that they do not introduce viruses, malware or malicious codes onto the Training Centre's systems.
- Not install or download from the internet any software without it first being checked for viruses.
- Staff should speak to the Head Of Training Centre for more information and guidance on appropriate steps to be taken to ensure compliance.

Communications and Transfer of Information

When speaking in public places (e.g. when speaking on a mobile phone), Staff and learners must take care in maintaining confidentiality.

Confidential Information must be marked 'strictly private and confidential' and circulated only to those who need to know the information during the course of providing training services to learners.

Confidential Information must not be removed from the Training Centre's offices (and systems) unless required for authorised business purposes, and then only in accordance with the subsequent paragraph.

If the transfer of Confidential Information from the Training Centre's offices is permitted, all reasonable steps must be taken to maintain the confidentiality and integrity of the information. This includes, but is not limited to, Staff ensuring that Confidential Information is:

- Stored with strong password protection, which is kept locked when not in use;
- Not transported in see-through or other unsecured bags or cases, when in paper copy;
- Not read in public places when working remotely (e.g. in waiting rooms or on trains); and
- Not left unattended or in any place where it is at risk.

Care must be taken to verify all postal and email addresses before any information is sent to them. Particular care must be taken when checking and verifying email addresses where auto-complete features may have inserted incorrect email addresses.

Before being sent by email or recorded delivery, all sensitive or particularly confidential information should be encrypted.

Personal Email, Cloud Storage Accounts and Highfields E-Learning Portal

Personal email accounts (e.g. Google, Hotmail and Yahoo) and cloud storage services (e.g. Google Drive, iCloud and OneDrive) are vulnerable to hacking and do not provide the same level of security as the services provided by the Employer's IT systems.

Staff must not use personal email accounts or cloud storage accounts for work purposes.
If large amounts of data need to be transferred, Staff should speak to the Head of Training Centre.

Transfer to Third Parties

Third party service providers (unless authourised, such as awarding organisation) should only be engaged to process information where appropriate written agreements are in place to ensure that they offer appropriate data protection, confidentiality and information security protections and undertakings. Care must be taken to consider whether any such third party service providers will be considered data processors for the purpose of the UK GDPR.

Staff involved in the process of setting up new arrangements or altering existing arrangements with third parties should speak to and consult with the DPO or the Head Of Training Centre for more information and guidance.

Training

The Training Centre will provide training on the concepts and measures contained in this policy to all learners at the start of each course, to staff as part of the induction process and at regular intervals thereafter or whenever there is a substantial change in the law or our policies and procedures.

Training is provided to staff online and through seminars or workshops. The completion of such training is compulsory. The Training Centre will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or this policy, please contact the DPO or the Head of Training Centre.

Reporting Data Breaches

All Staff are under an obligation to report actual or potential data protection compliance breaches to enable the Training Centre to:

- Investigate the breach and take any necessary remedial actions;
- Maintain a register of compliance breaches; and
- Make any applicable notifications (e.g. to the Information Commissioner's Office).

For more information on the Training Centre's reporting procedure, contact Clark Edwards, Head of Training Centre.

Consequences of Non-Compliance

The Training Centre takes compliance with this policy very seriously and failure to comply with this policy puts Staff, Learners and the Training Centre alike at significant risk.

Due to the importance of this policy, failure to comply with any of its procedures and requirements may result in disciplinary action and dismissal.

If you have any questions or concerns about anything in this policy, please contact the DPO (Clark Edwards) at info@SSIG-UK.co.uk.