MGT Information Security Policy for Modern Apprentices, Clients, Employers and Employees

Background and Purpose

The purpose of this document is to outline the required behaviour of MGT Training Ltd and their staff when using the MGT Training Ltd IT systems and handling MGT's personal data. The rules are defined to protect the interests of MGT, one of the organisations contracted to deliver National Training Programmes publicly and commercially on behalf of our participants. The intention is not to impose intrusive constraints that are contrary to MGT's established culture of openness, trust and integrity, which MGT recognise as essential contributors to the success of MGT. Information Security is committed to protecting the operation and reputation of MGT in fulfilling its role as the catalyst for real and positive change in Scotland's skills performance.

Responsibility

MGT is responsible for implementing, enforcing and adhering to the provisions of this policy.
All MGT signatories are responsible for ensuring this policy is adhered to.
All company employees are responsible for ensuring visitors are also aware of this policy and are supervised appropriately.

Policy

Any MGT employee (sub-contractor) in breach of this policy will be in breach of their contract with MGT and themselves may have their contract terminated.

Policy Statements

1 MGT IT System Access

1.1 The SDS IT systems are accessed using the provider's own individual MGT login ID and password. Do not leave clues or evidence of passwords near to the computer on which the information is being processed. Passwords should be minimum of 8 characters and include at least 3 of the following:

- Capital Letter
- Small letter
- Number character
- Special character (?$%&*)

1.2 Using another person's login ID **is not permitted** under any circumstances.
1.3 Some MGT IT systems require the use of multi factor authentication. This relies on additional security of a separate device / system such as a mobile phone or email account. In the event that the separate system is compromised, or the device lost, employees must notify MGT.
1.4 Passwords must not be saved on any login screen, e.g. do not tick 'Save Password' or 'Remember Me' options if these appear.
1.5 Never leave a logged-in computer unattended when using MGT IT systems. Use the Windows (or operating system equivalent) 'Lock Workstation' facility (Windows key + L) or logout.
1.6 Protect against accidental compromise of MGT and participant information; ensure information cannot be observed by unauthorised people.
1.7 Deliberate, unauthorised entry to MGT IT systems, entry of false data and unauthorised changes to information are strictly forbidden.
1.8 Employees must report all security incidents. In the first instance, employees must contact their MGT team leader who will ensure the correct handling of the incident.
1.9 Data extracted or originating from MGT IT systems must be encrypted or transferred in a secure manner when forwarding to MGT.
1.10 Employees must promptly inform MGT if they no longer need access to MGT systems.
1.11 Employees are required to comply with the terms of the User Permission arrangements in place between them and MGT.

2 Electronic Data Transfer – Mandatory Data Encryption

2.1 Data Encryption is a mandatory requirement of MGT where personal data is being transferred from and to third party organisations including providers. All data transfers between MGT and MGT and/ or third parties must use 256 bit AES encryption to encrypt files. Each data transfer will be to an individual's email address by means of an encrypted Zip file using a shared encryption password which must be changed on an annual basis. The password must not be transmitted by the same means as the encrypted data file. For example, if the encrypted data file is sent by email the password should be sent by instant message, text or by telephone call. Data transferred back to MGT must also be encrypted and follow the same process as set out above. If encrypted files are not available, hard-copy documents must be posted by using double envelopes.
2.2 Each provider must ensure that any portable devices, such as Laptops and Tablets, which are used to store participant's personal information are encrypted.
2.3 It is the responsibility of each employee to use the following free applications:

Windows users – https://7ziphelp.com

Mac users - https://izip.com

Failure to do so will result in a breach of employee contract and your contract maybe terminated.

3 Handling Hardcopy Documents and Electronic Media containing Personal Information

3.1 Employees are required to collect and store both personal information and special category personal information as defined by the Data Protection Act. This information must be securely protected to avoid the risk of data loss and unauthorised exposure.

4 Collecting

4.1 Personal information particularly 'special category' information must only be gathered from participants in an environment that respects their privacy and limits the opportunity for the participants to be overlooked.

5 Processing

5.1 When an employee processes a participant's personal data it should be done in a way to limit the opportunity for unauthorised access to the information.
5.2 Employees should consider protecting participant's information from unauthorised viewing by:

- Observing a clear desk policy
- Handling the hard copy in a non-transparent folder
- Ensure documents are not left in printers or copiers
- Ensure only authorised staff have access to the information.

6 Storage

6.1 When not in use hardcopy files with personal information must be stored in lockable filing cabinets or drawers.
6.2 At the end of the working day the filing cabinets and drawers containing the participant's personal information must be locked.

7 Sending

7.1 The preferred option for transferring personal information between parties is to use encrypted electronic communications as defined above in the section *Electronic Data Transfer – Mandatory Data Encryption.* If this is not available hardcopy documents can be exchanged either by post using double envelopes or hand delivered.

8 Disposal

8.1 Prior to disposal of information, employees should check the retention and archiving requirements.

8.2 Hardcopy documents that are no longer required should be shredded or disposed of via a confidential waste contractor.
8.3 For electronic storage media these should be destroyed or overwritten sufficiently such that the data cannot be retrieved.

- CD/DVD’s
- Memory sticks must be returned to MGT along with all equipment

9 Data Loss or Compromise

9.1 Any incident of data being lost or compromised must be reported promptly by the employee to a team leader within MGT