# Information Security Policy

**Introduction**

Focal Point Training and Consultancy Ltd is committed to preserving the confidentially, integrity and availability of information (see note below) we hold and to protecting the information from a range of threats, in order to ensure business continuity, minimise business damage or damage to individuals.

Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video.

***Note:*** *Confidentiality: ensuring that information is accessible only to authorised individuals.*

*Integrity: safeguarding the accuracy and completeness of information and processing methods.*

*Availability: ensuring that authorised users have access to relevant information when required.*

**We ensure that**

- ☑ Regulatory and legislative requirements will be met
- ☑ Our business continuity plan and information asset log are maintained and reviewed on an annual basis
- ☑ Regular information security briefings and updates will be available to all team members
- ☑ All associate team members are clear what processes to follow when handling information and data on behalf of Focal Point
- ☑ All breaches of information security, actual or suspected, will be reported to, and investigated by, the Directors (see data breach management process below)
- ☑ Our information asset log details what type of data is held where with security levels and access rights
- ☑ We ask for evidence of GDPR compliance for all new suppliers
- ☑ We delete data in line with our retention policy (see data protection policy and privacy notice)
- ☑ We ask for explicit consent or use legitimate interest as the lawful right to use any direct marketing to contacts on our database and reconfirm consent every 2 years

**Responsibilities**

1 All consultants are directly responsible for implementing the Information Security Policy within their sub contracted roles
2 It is the responsibility of each consultant to adhere to the Information Security Policy and we will check compliance at each annual review

## Company Information, Systems and Security – Guidelines for Team Members

1 The systems and data used by the Company are essential to the business, operations and management of the Company. The points made below must be observed, to protect the integrity of the Company's data and systems, to ensure that the company complies with its legal obligations, and to promote good business practice throughout the Company.
2 Systems and data are used solely for the purpose of the Company's business.
3 Systems and data are used only for the purpose of the Consultants' usual duties or for other purposes authorised in writing by the Company.
4 The physical security of the systems and data shall be maintained at all times.
5 Each consultant is required to store any Focal Point information on an encrypted data stick. Once the project they have been contracted for has finished, the consultant will email any information, such as training materials, coaching notes and action plans to our support manager, in order that they can be stored securely. Such data should then be deleted from the data stick. Any personal data will then be held in line with our retention policy.
6 Each consultant is responsible for ensuring they have suitable and up to date anti-virus/firewall software for their own systems (such as laptops, PCs and mobile devices), that all systems they use are password protected and that up to date security patches are applied regularly.
7 Associate consultants should keep to a minimum the data they carry on their data stick.
8 Associate consultants should maintain a clear desk policy to minimise risk of data breaches.
9 Any coaching notes or materials sent to a client should be in a PDF format.

10 Associate Consultants must use the Focal Point email address set up for them, when communicating with clients, delegates or other parties on Focal Point business.
11 Information discussed with clients by email or text should be factual and kept to a minimum. It is preferable to hold discussions by phone or face to face wherever possible.
12 Personal details should not be discussed in the body of an email. Information which contains personal data, such as coaching notes or actions from workshops should be written up in our Focal Point templates to be sent to the relevant parties and to our support manager for secure storage. (Please also see our coaching agreement issued to coaches).
13 Personal data relating to any client project will be held on our cloud based back up system, in line with our retention policy and then destroyed.
14 If a client contacts an associate consultant via their personal or their own company email address, they should direct the client back to their Focal Point email and inform Focal Point's support manager.
15 We check compliance with this policy at each annual one to one review and ask each associate consultant to sign that they comply.
16 Associate consultants should familiarise themselves with their responsibilities in relation to our Internal quality assurance policy, data protection policy and privacy notice.

## Data Breach Management Process

If a breach is identified by us or a 3rd party we will take the following steps:

### 1 Containment and recovery

One of the Directors will lead on investigating the breach

**We will**

- ☑ immediately deal with the data breach and take steps to prevent further loss of data
- ☑ identify who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment and recovery exercise. This could be finding a lost piece of equipment or recovering files from back up storage for example
- ☑ if appropriate, inform the police.

## 2 Assessing the Risk

We will initially assess the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

**This will include considering the following**

- ☑ What type of data is involved?
- ☑ How sensitive is it?
- ☑ If data has been lost or stolen, are there any protections in place such as encryption?
- ☑ What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- ☑ What could the data tell a third party about the individual? Could it be used in fraud or identity theft for example
- ☑ How many individuals' personal data are affected by the breach?
- ☑ Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach
- ☑ What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- ☑ Are there wider consequences to consider such as a loss of client confidence in an important service we provide?

## 3 Notification of breaches

- ☑ If we assess that there is a need to notify individuals affected, we will notify them and the ICO within 72 hours, where feasible
- ☑ This will include details of how and when the breach occurred and what data was involved and what we have already done to respond to the risks posed by the breach
- ☑ We will also try and give clear advice on the steps individuals can take to protect themselves and also what we can do to help

## 4 Evaluation and response

- ☑ We will investigate why the breach occurred and make recommendations as a result
- ☑ We will ensure recommendations are implemented in a timely way
- ☑ We document our response to and handling of a specific breach using our Data Breach Management spreadsheet
- ☑ We will review this process annually, along with our business continuity plan

## Communicating the Policy

We ensure that all our associate trainers and support staff have a copy of this policy when they first join our team. All staff will attest annually to their compliance with our data protection and IT policies.

## Reviewing the Policy

This policy will be monitored and reviewed annually.