
# Information Security Policy

## Aims

Information we collect, store and process may be subject to theft, misuse, loss or corruption. This policy is designed to identify the controls we have in place.

This policy applies to both staff and volunteers.

## Responsibilities

All staff who process information must ensure they not only understand but also act in line with this policy and the data protection policy.

Breach of this policy or unauthorised disclosure may result in disciplinary or legal action being taken.

## Data Storage

The company operates predominantly online, consisting of:

- Main websites
- OneDrive storage

All online sites are stored and backed up on EU based servers.

The company uses Microsoft Office 365 for email and OneDrive for data files, which are also stored locally on a computer and backed up to an off-site backup system. This enables the company to be able to guarantee data access from one of the three storage points at any time.

## Computer and Network security

All staff are required to use password protected devices that are protected from viruses and malware, to access their Microsoft Office 365 accounts, including if they are home or mobile working. Unsecured WiFi networks are not to be used (i.e. a WiFi network must be secured and

accessed with a password). We do not have a network and so we there are no separate arrangements in place for network security.

## Data access

Only authorised persons are allowed to access personal data. The company uses Microsoft OneDrive to store the majority of our data (explained above). Access privileges are authorised on a per user basis by the CEO and users are verified members of staff (i.e. their identity has been confirmed during their recruitment process).

## Data sharing

Data is collected from applicants to apply for the accreditation. Predominantly assessors are internal members of staff, however there may be occasions that we use an external contractor. These contractors are required to comply with our data protection policy and this policy.

## Data transmission

Personal data is transmitted using secure methods, such as temporarily sharing online access to files for the purpose of the accreditation. They are not able to download copies of the files and access is only allowed for the period of the assessment.

## System assurance and monitoring

Data usage and suspicious activity are automatically monitored within Microsoft Office 365. The software contains built in protection malicious software, such as malware, in addition all devices accessing company data are protected by anti-virus/malware software.

Suspicious activity on user's accounts will automatically suspend users to protect data. Warnings and events are logged and investigated and actioned within 12 hours of being flagged up.

## Risk management

A risk assessment of data and IT has been undertaken and is reviewed every 12 months, or more frequently if a threat is identified. This covers risks of malware, staff mistakes and criminal activity. This risk assessment and the annual review is approved by the Director.

## Compliance

Information systems used by the company must be compliant with all statutory, regulatory and contractual security requirements. Examples include GDPR and contractual agreements.

## Review

This policy will be reviewed annually by the CEO.

December 2020