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.

Staff 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.

Public spaces

Unsecured public or private WiFi networks are not to be used (i.e. a WiFi network must be secured and accessed with a password).

Sensitive data, such as personal details, must not be accessed in public places where the document or device can be viewed by others.

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).

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. Passwords are required to be at least 8 characters long with a combination of letters, symbols and numbers and should not contain whole words. We do not have a network and so we there are no separate arrangements in place for network security.

Data transmission

Personal data is transmitted using secure methods, such as direct email, Egress secure emails, sharing OneDrive direct links or secure file sharing software.

Company Responsibilities

Digital Data Storage

The company operates predominantly online, consisting of:

- Main websites
- Facebook groups – private support groups for attendees of courses and also trainers to enable them to seek support from peers
- 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.

Removable media will not be used for the storage of protected data and secure methods should be used for the transmission of data as outlined under Data Transmission.

Physical records

Physical paperwork is minimised and the use of digital files is encouraged. Physical paperwork is stored in a locked filing cabinet within our coded access storage facility. This can only be accessed with the approval of the CEO and key fob access is required to the building, plus code for the storage room and key for the filing cabinet.

Data sharing

For regulated qualifications, data is shared with both the awarding body and in England, the Education Skills and Funding Agency in order to administer the provision and assessment of the qualification.

For funded training, data is also shared with the funding bodies in order to be able to evidence and claim funding.

Payment processing

On occasion customers may choose to pay us by card (such as a purchase through the website) or direct debit (such as monthly instalments for licence fees). We use Stripe and GoCardless respectively for these transactions. Only the CEO has access to these accounts and they do not provide access to customer card or bank account information.

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, the payment card industry standard (PCI-DSS) and contractual agreements.

Accreditation

The company complies with and holds the CyberEssentials Plus accreditation mark.

Review

This policy will be reviewed annually by the CEO.

September 2024