Staff Power Training Online Safety Policy

Policy Statement:

At Staff Power Training, we are committed to providing a safe online environment for all employees, clients, and partners. Online safety is a top priority for us, and we aim to maintain the privacy, security, and integrity of all online activities within our organisation.

Purpose:

This policy aims to outline the guidelines and best practices for ensuring online safety while engaging in any online activities related to Staff Power Training. It is designed to protect confidential information, prevent security breaches, and promote responsible online behaviour.

Scope:

This policy applies to all employees, contractors, clients, partners, Learners and third parties who have access to Staff Power Training's online resources, including but not limited to email communication, internal systems, and collaboration platforms.

Policy Guidelines:

1. Confidentiality:
   - All employees are required to maintain the confidentiality of sensitive information exchanged online. This includes but is not limited to client data, financial information, and internal communications.

2. Password Security:
   - All users must follow strong password practices, including creating complex passwords, changing them regularly, and not sharing them with others. Multi-factor authentication is highly encouraged for added security.

3. Phishing Awareness:
   - Employees should be vigilant against phishing attempts and report any suspicious emails or communications to the IT department immediately. Staff Power Training will conduct regular training sessions to educate employees on identifying and avoiding phishing attacks.

4. Data Protection:
   - All data stored online must be protected and encrypted where possible. Employees are responsible for ensuring the security of any data they handle and adhering to data protection laws and regulations.

5. Safe Internet Usage:
   - Employees are expected to use the internet responsibly and professionally while representing Staff Power Training online. This includes refraining from accessing inappropriate websites, downloading unauthorised software, or engaging in online activities that may compromise security.

Responsibilities:

- The IT department is responsible for implementing and maintaining online security measures, monitoring online activity, and responding to security incidents.
- All employees are responsible for familiarising themselves with this policy, adhering to its guidelines, and reporting any online safety concerns to the appropriate authorities.

Policy Owner:
Lee Johnston, Director of Quality, is the designated owner of this policy and is responsible for its enforcement, implementation, and review.

January 2024 V1
Next due for review January 2025