IT, Computer, Social Media, and Surveillance Policy

Purpose

Lifelong Healthcare expects all employees to maintain a professional standard of behaviour when using the company's computer systems, internet, and social media. This policy provides a clear framework outlining expectations and rules related to IT usage to ensure security, compliance, and professionalism. Employees must also adhere to responsible behaviour when using social media for both work-related and personal purposes.

Internet Usage

Authorised employees may use the internet for professional activities relevant to their role. However, the following activities are strictly prohibited:

- Accessing websites that could expose Lifelong Healthcare to security threats, copyright issues, or intellectual property violations.
- Engaging in social media activities that breach Lifelong Healthcare's social media policy.
- Downloading, posting, or sharing any content unrelated to work, including offensive or inappropriate material.
- Participating in hacking, security breaches, or any activity that compromises Lifelong Healthcare's IT security.

Any employee found engaging in these activities may be subject to disciplinary action, up to and including dismissal. Certain internet activity may also constitute a criminal offence.

Monitoring and Compliance

Lifelong Healthcare reserves the right to monitor and review employee use of IT systems, including:

- Internet activity, including websites visited and time spent online.
- Email communications sent and received through the company's network.
- Downloaded or uploaded material.

Monitoring aims to ensure compliance with policies and regulatory requirements. Any information obtained may be used in disciplinary proceedings if violations are found.

Social Media Usage

Employees must not post work-related content or any material that could identify customers, clients, or colleagues in a manner that negatively impacts Lifelong Healthcare. This always applies, whether during or outside working hours, and includes access via mobile devices.

Use of Computer Equipment

To safeguard company systems and data security:

- New software must be reviewed and authorised by management before use.
- Only business-related software may be installed on Lifelong Healthcare devices.
- No unauthorised software, devices, or data may be transferred to or from company premises.
- Unauthorised access to company computing facilities will result in disciplinary action, up to and including dismissal.
- Copying or removing company-owned software or hardware without authorisation is strictly prohibited.

Surveillance Policy

Lifelong Healthcare may use CCTV surveillance to ensure workplace safety and security. CCTV footage may be reviewed and used in disciplinary proceedings if necessary. Cameras will be placed in visible locations and will not be installed in private areas such as restrooms or changing rooms.

Employee Acknowledgment

By signing below, you confirm that you have read, understood, and agree to abide by this IT, Computer, social media, and Surveillance Policy.

Employee Name: _____

Employee Signature: _____ Date: _____

HR Contact or Supervisor: _____