STAFFING MATCH

BRINGING YOUR OWN DEVICES TO WORK

2017

Staffing Match
Bringing Your Own Devices to Work

1. Introduction

This policy applies to employees who work remotely or who bring their computers and/or other electronic devices, such as smartphones, mobile phones and tablets into work. This **Policy on Bringing Employees' Own Devices to Work** (BYOD) is intended to protect the security and integrity of any personal data and the Company's technology infrastructure. It should be read in conjunction with the Company's **Communications, Email and Internet Policy.**

With the prior agreement of the Director of Finance, All employees are permitted to use their own devices for work-related purposes. However, employees must agree to the terms and conditions set down in this policy in order to be able to connect their devices to the company network.

2. Acceptable Use

The employee is expected to use his or her devices in an ethical manner at all times in accordance with the Company's **Communications, Email and Internet Policy.**

The company defines acceptable use of employee's own devices as:

Devices' camera and/or video capabilities must be disabled while on-site.

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- Engage in outside business activities

Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, and documents.

Employees should be aware that any personal device used at work may be subject to discovery in litigation and may be used as evidence in any action against the Company.

3. Data Protection Act

The Data Protection Act 1998 requires the Company to process any personal data in accordance with the eight data protection principles (see the Company's separate Data Protection Policy). 'Processing' includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and disposing of it. This policy applies, in particular, to the seventh data protection principle which requires the Company to ensure that personal data is protected by appropriate technical and organisational measures against unauthorised or unlawful processing or disclosure and against accidental loss, damage or destruction.

4. Employees' Obligations in respect of BYOD

4.1 Security

- In order to prevent unauthorized access, devices must be password protected using a strong password
- Any device used must lock itself with a password or PIN if it is idle for five minutes
- Any device used must be capable of locking automatically if an incorrect password is entered after several attempts
- Employees must ensure that, if they transfer data, they do so via an encrypted channel e.g. a VPN
- Employees must not download unverified apps that may present a threat to the security of the information held on their devices
- Employees should not use unsecured networks
- The loss of a device used for work-related activities must be reported at the earliest opportunity to <<insert job title e.g. the IT Manager>>.

4.2 Devices and Support

- Devices must be presented to <<insert job title e.g. the IT Manager>> for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before employees can access the network.

4.3 Retention of Personal Data

- Employees must not keep personal data for longer than necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer in order to comply with a legal obligation.

4.4 Deletion of Personal Data

- Employees must ensure that, if they delete information from a device, the information must be permanently deleted rather than left in the device's waste management system.

- If removable media, e.g. a USB drive or CD, is used to transfer personal data, employees must ensure that the personal data is deleted after the transfer is complete.

4.5 End of Employment

- Prior to the last day of employment with the Company, all employees must delete work-related personal data on his/her own device.

4.6 Third-Party Use of Devices

- Employees must ensure that, in the event of friends or family using their devices, they are not able to access any work-related personal information by, for instance, password-protecting the information.

5. Monitoring

The Company will monitor data protection compliance in general and compliance with this policy in particular. Before any monitoring is undertaken, the Company will identify the specific purpose of the monitoring.

The Company shall ensure that any monitoring of communications complies with the Data Protection Act 1998.

6. Non-Compliance

Any employee found to be breaching this policy will be treated in line with the Company's usual disciplinary procedure. Breaches of this policy could result in disciplinary action up to, and including, dismissal. Employees should be aware that they may incur personal criminal liability for breaches of this policy.

7. Review

This BYOD policy will be reviewed on an annual basis.

This policy has been approved & authorised by:

Name: <<Insert Full Name>>

Position: <<Insert Position, e.g. Human Resources Manager>>

Date: <<Date>>

Signature: