Company Name

Policy on Bringing Employee's Own Devices to Work (*BYOD*)

Last updated date:

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 [***insert name and job title***], all**]**/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 and Data Protection Policy.

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

- activities that directly or indirectly support the business of the Company
- [reasonable and limited personal communication or recreation, such as reading or game playing.]

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, [***include any other***] 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 (see also 5.3 below).

The General Data Protection Regulation (*GDPR*)

[***Insert Company Name***] is the data controller in respect of work-related personal data that is held on personal devices. [***Insert name and job title***] is the Company's data protection officer and is responsible for the implementation of this policy.]

The GDPR requires the Company to process personal data in accordance with the six data protection principles. Employers must:

- Process personal data fairly, lawfully and transparently
- Obtain and process data only for one or more specified and lawful purposes
- Ensure that data is adequate, relevant and limited to what is necessary
- Ensure that data is accurate and kept up-to-date
- Not keep data longer than necessary
- Take appropriate technical and organisational measures against accidental loss or destruction of, or damage to, personal data.

3. Special Category Data

"Special category data" is information about an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or philosophical beliefs
- trade union membership
- physical or mental health or condition
- sex life or sexual orientation.

EITHER

[Employees must not process special category data on a personal device. If an employee has any special category data on his or her device, he or she must have it permanently deleted from the device.]

OR

[Employees may store special category data on a personal device provided that the device has a sufficiently high level of encryption.]

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 name and job title***]

- Employees must report data breaches to ***insert name and job title***] immediately.

4.2 ***Devices and Support***

- Devices must be presented to ***insert name and job title***] 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 **Cooperation with subject access requests**

Any individual whose personal date is held by the Company has the right to make a subject access request. Consequently, the Company may have to access your device in order to retrieve any data that is held on it about the individual. You must allow the Company to access the device and carry out a search for information about an individual that may be held on the device.

4.4 **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.

4.5 **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.

4.6 **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.

4.7 **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

As part of its obligations under the GDPR, the Company will monitor data protection compliance in

general and compliance with this policy in particular. The monitoring is in the Company's legitimate interests to ensure compliance with this policy and to ensure that the Company is complying with its obligations under the GDPR.

Before any monitoring is undertaken, the Company will identify the specific purpose of the monitoring.

Monitoring will consist of: [***insert methods of monitoring***].

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 and Training

The Company will provide data protection training to all employees on a regular basis.

This BYOD policy will be reviewed on an annual basis.

This policy has been approved and authorised by:

Name:

Position:

Date:

Signature:

In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of the documents.