

Policy on Bringing Employee-Owned Devices to Work (BYOD)

1. Introduction

This policy applies to employees who bring their computers and/or other electronic devices, such as mobile phones and tablets into work. This **Policy on Bringing Employee-Owned Devices to Work (BYOD)** is intended to protect the security of any personal data and the Company's technology infrastructure in conjunction with the Company's **Communication Policy**.

[With the prior agreement of the IT Manager>>, all] All employees are permitted to use their own devices for work-related purposes. However, employees must adhere to the conditions set down in this policy in order to be able to connect to the company network.

2. Acceptable Use

The employee is expected to use devices in an ethical manner at all times in accordance with the **Acceptable Use Policy** and **Data Protection Policy**.

The company defines acceptable use of employee-owned devices as:

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

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

Devices may not be used at work for the following purposes:

- Store or transmit illicit material
- Store or transmit proprietary information to another company
- Harass others
- [Engage in outside business]

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

Employees should be aware that data stored on devices used at work may be subject to discovery in litigation and used as evidence in any action against the Company (see also the **Acceptable Use Policy**).

3. The General Data Protection Regulation

<<State Company Names>> is the name of the company and job title>> is the Company's data protection policy.]

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

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

4. Special Category Data

"Special category data" is information relating to an individual's:

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

EITHER

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

OR

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

5. Employees' Obligations in relation to Data Protection

5.1 Security

- In order to prevent unauthorized access, all devices must be password protected using a strong password
- Any device used must be locked with a password or PIN if it is idle for five minutes

S

- Any device used must be locked automatically if an incorrect password is entered
- Employees must ensure that all data, they do so via an encrypted channel e.g. a VPN
- Employees must not use devices that may present a threat to the security of the information devices
- Employees should not use public Wi-Fi networks
- The loss of a device must be reported at the earliest opportunity to the IT Manager>>
- Employees must report the loss of a device to the IT Manager>> immediately

A

5.2 Devices and Support

- Devices must be properly configured (e.g. the IT Manager>> for proper job provisioning) and standard apps, such as browsers, must be installed before employees can access the network.

M

5.3 Cooperation with subject

- Any individual whose device is subject to a search by the Company has the right to make a subject access request. If the Company may have to access your device in order to carry out a search for information, the Company may have to access the device and carry out a search for information that may be held on the device.

5.4 Retention of Personal Data

- Employees must not retain personal data for longer than necessary for the purpose for which it is collected. There is a requirement to retain it for longer in order to comply with the law.

P

5.5 Deletion of Personal Data

- Employees must ensure that personal data is deleted from a device, the information must be deleted from the device's waste management system
- If removable media, such as USB drives, is used to transfer personal data, the data is deleted after the transfer is complete.

5.6 End of Employment

- Prior to the last day of employment, all employees must delete work-related personal data from their own device.

5.7 Third-Party Use of Devices

- Employees must ensure that personal data is not shared with friends or family using their devices, they are not to share work-related personal information by, for instance, password protection.

L

E

S

6 Monitoring

As part of its obligations under the law, the Company will monitor data protection compliance in general and data protection in particular. The monitoring is in the Company's legitimate interest to ensure compliance with this policy and to ensure that the Company is compliant with the provisions under the GDPR.

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

Monitoring will consist of: <<

any will monitor data protection compliance in particular. The monitoring is in the Company's legitimate interest to ensure compliance with this policy and to ensure that the Company is compliant with the provisions under the GDPR.

will identify the specific purpose of the monitoring.

7 Non-Compliance

Any employee found to be in breach of this policy will be treated in line with the Company's usual disciplinary procedures. 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.

Any employee found to be in breach of this policy will be treated in line with the Company's usual disciplinary procedures. 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.

8 Review and Training

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

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

This BYOD policy will be reviewed annually.

s.

This policy has been approved & authorised by the Board of Directors.

Name: <<Insert Name>>

Position: <<Insert Position>>

Resources Manager>>

Date: <<Date>>

Signature:

A

M

P

L

E