Policy on Bringing Em ces to Work (BYOD)

1. Introduction

This policy applies to emplo or who bring their computers and/or other electronic devic s, mobile phones and tablets into work. This **Polic es' Own Devices to Work** (BYOD) is intended to prote ty of any personal data and the Company's technology infra ad in conjunction with the Company's **Communicatio Policy.**

[With the prior agreement of IT Manager>>, al**l]** All employees are permitted to r work-related purposes. However, employees must a nditions set down in this policy in order to be able to he company network.

2. Acceptable Use

The employee is expected t n an ethical manner at all times in accordance with the ations, Email and Internet **Policy** and **Data Protection**

The company defines accep own devices as:

- activities that directly or siness of the Company
- [reasonable and limited or recreation, such as reading or game playing.]

Devices' camera and/or vide sabled while on-site.

Devices may not be used at

- Store or transmit illicit m
- Store or transmit proprie g to another company
- Harass others
- [Engage in outside busi

Employees may use their m e following company-owned resources: email, calendars, >>] and documents.

Employees should be aware e used at work may be subject to discovery in litigat evidence in any action against the Company (see a

3. The General Data Protecti

<<State Company Names>> respect of work-related personal data that is held on persona e and job title>> is the Company's data protection o for the implementation of this policy.]

The GDPR requires the Co al data in accordance with the six data protection principles. E

- Process personal da sparently
- Obtain and process specified and lawful purposes
- Ensure that data is a nited to what is necessary
- Ensure that data is a ate
- Not keep data longe
- Take appropriate tec measures against accidental loss or destruction o data.

4. Special Category Data

"Special category data" is in dual's:

- racial or ethnic origin
- political opinions
- religious beliefs or p
- trade union member
- physical or mental h
- sex life or sexual orie

EITHER

[Employees must not process spec rsonal device. If an employee has any special category data on h e must have it permanently deleted from the device.]

OR

[Employees may store special cate device provided that the device has a sufficiently high level of encry

5. Employees' Obligations in

5.1 Security

- In order to prevent u ices must be password protected using a strong passw
- Any device used mu ord or PIN if it is idle for five minutes

- Any device used mu… automatically if an incorrect password is entered …
- Employees must ens… data, they do so via an encrypted channel e.g. a VPN
- Employees must not … s that may present a threat to the security of the int… evices
- Employees should n… ks
- The loss of a device … tivities must be reported at the earliest opportunity t… e IT Manager>>
- Employees must rep… nsert job title e.g. the IT Manager>> immedia…

5.2 Devices and Suppor…

- Devices must be pre… e e.g. the IT Manager>> for proper job provisioni… tandard apps, such as browsers, office productivity so… before employees can access the network.

5.3 Cooperation with sub…

- Any individual whose … the Company has the right to make a subject acce… y, the Company may have to access your device i… ta that is held on it about the individual. You must… ccess the device and carry out a search for informatio… may be held on the device.

5.4 Retention of Persona…

- Employees must not … onger than necessary for the purpose for which it i… re is a requirement to retain it for longer in order to co… on.

5.5 Deletion of Personal…

- Employees must ens… formation from a device, the information must be … er than left in the device's waste management system…
- If removable media, … s used to transfer personal data, employees must ens… a is deleted after the transfer is complete.

5.6 End of Employment …

- Prior to the last day … e Company, all employees must delete work-related p… own device.

5.7 Third-Party Use of D…

- Employees must ens… riends or family using their devices, they are not… -related personal information by, for instance, passwo… tion.

6 Monitoring

As part of its obligations unc any will monitor data protection compliance in general and c y in particular. The monitoring is in the Company's legitimate liance with this policy and to ensure that the Company is tions under the GDPR.

Before any monitoring is unc ill identify the specific purpose of the monitoring.

Monitoring will consist of: <<

7 Non-Compliance

Any employee found to be will be treated in line with the Company's usual disciplina s of this policy could result in disciplinary action up to, and mployees should be aware that they may incur personal crin s of this policy.

8 Review and Training

The Company will provide d all employees on a regular basis.

This BYOD policy will be rev s.

This policy has been approved & au

Name: <<Insert

Position: <<Insert sources Manager>>

Date: <<Date>>

Signature: