**[NAME OF ORGANISATION]**

1. Bring your own device to work policy
2. introduction

This policy applies where employees use their own smartphones, tablets or other mobile devices for work either while at the office, during working hours or during non-working hours.

This policy deals with acceptable use, information security and compliance with the principles of data protection law (as applicable), employees’ expectation of privacy, **[name of organisation]**’s right of access and issues surrounding technical support and responsibility for running costs.

1. ABOUT THIS POLICY

This policy covers all employees, workers, officers, consultants, contractors, [volunteers,] [interns,] casual workers and agency workers.

**[Name of organisation]** recognises that many of our staff have personal mobile devices (such as tablets, smartphones and handheld computers), which they could use for work purposes, and that there can be benefits for both **[name of organisation]** and staff, including increased flexibility in our working practices, in permitting such use. However, the use of personal mobile devices for work purposes gives rise to increased risk in terms of the security of our IT resources and communications systems, the protection of personal data, confidential and proprietary information and reputation, and compliance with legal obligations.

Anyone covered by this policy may use a personal mobile device for work purposes, provided that they sign the declaration at the end of this policy and adhere to its terms.

No one is *required* to use their personal mobile device for work purposes. It is a matter entirely for each person’s discretion.

*[This policy has been [agreed OR implemented following consultation] with the [[TRADE UNION] OR [WORKS COUNCIL] OR [STAFF ASSOCIATION]].]*

Certain obligations under this policy are contractual and if you are an employee or worker, will form part of your contract of employment or contract of service. These are clearly identified. The remaining sections of this policy do not form part of any contract of employment or contract of service and [name of organisation] may amend it at any time, including the contractual obligations that it places on staff, or remove the policy entirely, at any time.

1. PERSONNEL RESPONSIBLE FOR THIS POLICY

**[Name of organisation]**’s [SPECIFY e.g. board of directors] has overall responsibility for the effective operation of this policy [, but has delegated day-to-day responsibility for its operation to [POSITION]].

POSITION] [in conjunction with the [COMMITTEE] OR board of directors]] shall be responsible for reviewing this policy to ensure that it meets legal requirements and reflects best practice.

[SPECIFY] has responsibility for ensuring that any person who may be involved with administration, monitoring, IT security or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

All staff are responsible for the success of this policy. Any misuse (or suspected misuse) of a device or breach of this policy should be reported to [POSITION].

If you have any questions regarding this policy or have questions about using your device for work purposes which are not addressed in this policy, please contact [POSITION].

1. SCOPE AND PURPOSE OF THE POLICY

This policy applies to staff who use a personal mobile device including any accompanying software or hardware (referred to as a ‘device’ in this policy) for work purposes. It applies to use of the device both during and outside office hours and whether or not use of the device takes place at your normal place of work.

This policy applies to all devices used to access **[name of organisation]**’s IT resources and communications systems (collectively referred to as ‘systems’ in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, PDAs, tablets, and laptop or notebook computers.

When you access [name of organisation]’s systems you may be able to access data about **[name of organisation]** or [our associated/group companies and] individuals (such as [employees] [contractors] [members], [customers], [clients] [distributors], [suppliers] and, including information which constitutes personal data[[1]](#footnote-1) and/or is confidential, proprietary or private (collectively referred to as **organisational data** in this policy).

[Name of organisation] is a controller of the organisational data referred to in paragraph 16 above, as such, we must ensure that the processing of organisational data on any device remains in compliance with applicable data protection legislation, particularly in the event of a personal data breach.

When you access [name of organisation]’s systems using a device, we are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or organisational data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of organisational data (including personal data and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our organisation and our reputation.

The purpose of this policy is to protect **[name of organisation]**’s systems and data, and to prevent data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access **[name of organisation]**’s systems using a device. This policy sets out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.

Breach of this policy may lead to **[name of organisation]** revoking your access to our systems, whether through a device or otherwise. It may also result in disciplinary action up to and including dismissal [and in the case of a breach of this policy by a contractor, consultant, casual or agency worker, the termination of the engagement]. [It may also lead in some cases to possible criminal charges.]

Disciplinary action may be taken whether the breach of this policy is committed during or outside office hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into suspected breach of this policy, which may involve providing **[name of organisation]** with access to the device and any relevant passwords and login details.

Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist staff in connecting to our systems.

CONNECTING DEVICES TO OUR SYSTEMS

Connectivity of all devices is centrally managed by [SPECIFY], who **must approve** a device before it can be connected to our systems. Devices must comply with our IT Security Policy.

**[Name of organisation]** reserves the right to refuse or remove permission for your device to connect with our systems. [The IT Department OR [SPECIFY]] will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in [name of organisation]’s reasonable opinion a device is being or could be used in a way that puts, or could put, us, our staff, our systems, or our organisational data at risk or that may otherwise breach this policy.

[In order to access **[name of organisation]**’s systems it may be necessary for [the IT Department OR [SPECIFY]] to install software applications on your device. If you remove any such software, your access to our systems will be disabled.]

MONITORING

The contents of **[name of organisation]**’s systems and data are **[name of organisation]**’s property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of working or on [name of organisation]’s behalf is our property, regardless of who owns the device.

**[Name of organisation]** reserves the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device.

It is possible that personal data may be inadvertently monitored, intercepted, reviewed or erased. Therefore, you should have no expectation of privacy in any data on the device. Staff are advised not to use **[name of organisation]**’s systems for any matter intended to be kept private or confidential.

[**Name of organisation**] considers that the possible inadvertent processing of your personal data and the personal data of 3rd parties is necessary to ensure compliance with the data protection principles and has a legal basis for processing your personal data and the personal data of 3rd parties in this regard. See paragraphs [41] – [43].

SECURITY REQUIREMENTS

You must ensure compliance with applicable data protection law in relation to the organisational data you process on the device.

You must comply with **[name of organisation]**’s [IT Communications Systems Policy OR [SPECIFY POLICY]] which is available from [SPECIFY WHERE AVAILABLE] when using your device to connect to our systems.

In addition, [and to the extent our [IT Communications Systems Policy OR [SPECIFY POLICY]] does not address the issues below,] you must:

* + 1. at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, adequate strength passwords, encryption, and physical control of the device;
    2. install any anti-virus or anti-malware software at [**name of organisation**]’s request before connecting to our systems and consent to our efforts to manage the device and secure its data, including providing us with any necessary passwords;
    3. protect the device with a PIN number or password, and keep that PIN number or password secure at all times. The PIN number or password should be changed [regularly OR every [NUMBER] weeks]. If the confidentiality of a PIN number or password is compromised, you must change it immediately. The use of PIN numbers and passwords should not create an expectation of privacy by you in the device;
    4. maintain the device’s original operating system and keep it current with security patches and updates;
    5. [not download or transfer [any data OR [DESCRIBE RESTRICTED CATEGORIES OF DATA e.g. financial data, sensitive category data, employee personal data, the personal data of members]] to the device, for example via e-mail attachments, unless specifically authorised to do so. You must immediately erase any such information that is inadvertently downloaded to the device;]

[Name of organisation] reserves the right, without further notice or permission, to inspect your device and access data and applications on it, and remotely review, copy, disclose, wipe or otherwise use some or all of the organisational data on it for legitimate purposes, which include (without limitation) enabling us to:

* + 1. inspect any organisational data stored on the device or on backup or cloud-based storage applications;
    2. investigate or resolve any security incident or unauthorised use of our systems;
    3. conduct any relevant compliance obligations (including in relation to concerns regarding confidentiality, data protection or privacy); and
    4. ensure compliance with [**name of organisation**]’s rules, standards of conduct and policies in force from time to time (including this policy).

You must co-operate with [**name of organisation**] to enable such inspection, access and review, including providing any passwords or PIN numbers necessary to access the device or relevant applications. A failure to co-operate with us in this way may result in disciplinary action being taken, up to and including dismissal. This paragraph 34 of the policy is contractual.

If **[name of organisation]** discovers or reasonably suspects that there has been a breach of this policy, including any of the security requirements listed above, **[name of organisation]** shall immediately remove access to our systems and, where appropriate, remove any organisational data from the device. Although we do not intend to wipe other data that is personal in nature (such as photographs or personal files or e-mails), it may not be possible to distinguish all such information from organisational data in all circumstances. You should therefore regularly backup any personal data contained on the device.

[**Name of organisation**] considers that the possible inadvertent processing of your personal data and the personal data of 3rd parties is necessary to ensure compliance with the data protection principles and has a legal basis for processing your personal data and the personal data of 3rd parties in this regard. See paragraphs [41] – [43].

We will not track any personal devices via GPS or location based Wi-Fi without your or the device owner’s permission.

1. LOST OR STOLEN DEVICES AND UNAUTHORISED ACCESS

In the event of a lost or stolen device, or where a staff member believes that a device may have been accessed by an unauthorised person or otherwise compromised, the staff member must report the incident to [the IT Department OR [SPECIFY]] **immediately**.

[Any personal data breach with be addressed in accordance with [**name of organisation**]’s Personal Data Breach Reporting Procedure.]

1. PROCEDURE ON TERMINATION OF EMPLOYMENT

On your last day of work, or your last day before commencing a period of garden leave, all organisational data (including work e-mails), and any software applications provided by us for organisational purposes, will be removed from the device. If this cannot be achieved remotely, the device must be submitted to [SPECIFY] for wiping and software removal. You must provide all necessary co-operation and assistance to [SPECIFY] in relation to this process. This paragraph 40 of the policy is contractual.

1. PERSONAL DATA

In accordance with [**name of organisation**]’s rights under this policy to monitor (paragraph [27]), inspect (paragraph [34]) and secure the device (paragraph [40]), [name of organisation] may inadvertently process your personal data or the personal data of 3rd parties in the way outlined in those paragraphs.

[Name of organisation]’s purpose for processing personal data in this way is to:

* + 1. Prevent misuse of the device and organisational data;
    2. To ensure compliance with our rules and standards of conduct and policies in force from time to time (including this policy);
    3. To monitor performance at work; and
    4. To ensure that staff do not use our facilities and systems for any unlawful purposes or activities that may result in adverse consequences for [name of organisation].

[**Name of organisation**] considers that it has a legitimate interest in processing your personal data and the personal data of 3rd parties (albeit inadvertently) for the reasons outlined above. [**Name of organisation**] will use reasonable endeavours not to access, copy, monitor, intercept, review, wipe remove, erase or otherwise process your personal data or the personal data of 3rd parties. If such processing occurs [**name of organisation]** shall delete any and all such personal data as soon as it comes to our attention. This limitation does not apply to personal data which is also organisational data (including personal emails sent or received using [**name of organisation**]’s email system. For this reason, you are encouraged not to use work email for personal purposes.

1. APPROPRIATE USE

You should never access or use our systems or organisational data through a device in a way that breaches any of **[name of organisation]**’s other policies. For example, you must not use a device to:

* + 1. [breach **[name of organisation]**’s obligations with respect to the rules of relevant regulatory bodies;]
    2. [breach any obligations that relevant regulatory bodies may have relating to confidentiality and privacy;]
    3. [breach **[name of organisation]**’s Disciplinary Rules;]
    4. defame or criticise us or **[name of organisation]**’s [affiliates], [customers], [clients], [business partners], [suppliers], [vendors], [members] or [other stakeholders];
    5. [[harass or bully other staff in any way OR breach **[name of organisation]**’s Anti-harassment and bullying policy];]
    6. [[unlawfully discriminate against other staff or third parties OR breach **[name of organisation]**’s Equal opportunities policy];]
    7. [breach **[name of organisation]’**s Data protection policy;]

If you breach any of the above policies, you may be subject to disciplinary action up to and including dismissal.

1. TECHNICAL SUPPORT

We do not provide technical support for devices. If you use a device for work purposes you are responsible for any repairs, maintenance or replacement costs and services.

1. COSTS AND REIMBURSEMENTS

You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By signing the declaration at the end of this policy you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your work usage of the device may increase your voice and data usage charges.

1. DECLARATION AND AGREEMENT

I **[NAME]** wish to use my personal mobile device for work purposes and explicitly confirm my understanding and agreement to the following:

I have read, understood and agree to all of the terms contained in the Bring Your Own Device to Work Policy.

I understand that the terms of this policy will apply to me at all times, during or outside office hours and whether or not I am at my normal place of work.

I acknowledge and agree that authorised personnel of [**name of organisation**] shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my personal data).

I understand and agree that [**name of organisation**] in its discretion may amend, or remove this policy at any time and that I will be bound by the terms of the policy as amended.

|  |
| --- |
| ……………………………………………… |
| SIGNED |
|  |
| ……………………………………………… |
| PRINTED NAME  …………………………………………………  DATE |
|  |

1. As defined by data protection legislation (as applicable) [↑](#footnote-ref-1)