BYOD (Bring Your Own Device) Policy

Introduction

CompanyX is committed to flexible working and has a suite of flexible working policies and associated guidance and toolkits. Further, *CompanyX* recognises that Device owners wish to use their own mobile devices to access *CompanyX* data and use *CompanyX* applications as part of flexible working arrangements. This policy outlines the responsibilities of both the device owner and *CompanyX*.

This document provides standards and guidance for acceptable behaviour for the use of personal devices, such as smart phones and tablets, by *CompanyX* device owners to access network resources, namely their *CompanyX* e-mail, calendar, and MS Teams, for business purposes. This policy will be updated regularly to accurately reflect devices and IT Services coverage.

Access to and continued use of network services is granted on the condition that each device owner reads, signs, respects and follows *CompanyX* policies concerning use of these devices and services. The use of a personally owned device in connection with *CompanyX* business is a privilege granted to device owners through approval of Information Services management. *CompanyX* reserves the right to revoke these privileges if device owners do not abide by the policies and procedures set forth in this document.

What is Bring Your Own Device?

"Bring Your Own Device" (BYOD) refers to organisations permitting their device owners to bring personally owned mobile devices (e.g., tablets and smart phones) to their workplace, and use those devices to access privileged organisational information and applications.

Who does it apply to?

This policy applies to employees, contractors and third parties who wish to connect to any of *CompanyX* computer systems to access CompanyX electronic data using a personal device. Third parties would additionally be required to agree to the appropriate data sharing policies.

Device, Application or Data Access Limitations

The IT Services covered by policy are:

- E-mail – business e-mails are accessed, and three days' worth are downloaded to the device, after which they are overwritten
- Calendar
- Contacts
- Tasks
- MS Teams

These are subject to normal performance management constraints.

Who Manages this Service?

Information Services in conjunction with Corporate Governance will manage the BYOD facility, as described within this document, on behalf of *CompanyX*. Human Resources will advise managers if corporate policies have not been followed. In specific the BYOD facility includes the approval, monitoring, reporting and security incident processes, e.g., wiping the device, for all devices.

What Support will Information Services Provide?

CompanyX will not support or maintain any personal mobile device. Further, *CompanyX* will not cover any damage to the device. It is recommended that device owners insure their device as part of their home contents insurance and advise their insurer that the device will be used for work purposes at home and at work locations.

The device owner is personally liable for the device and carrier service costs. They will not be reimbursed by *CompanyX* for the acquisition of a mobile device, its use, maintenance or replacement or any carrier service charges incurred. The device owner must agree to all terms and conditions in this policy to be allowed access to the *CompanyX* services listed in this document.

CompanyX and Information Services specifically reserve the right to disable or disconnect some or all services without prior notification.

Device Owner Responsibilities

As the device owner, you carry specific responsibilities, as listed below:

- You will not lend anyone your device to access *CompanyX* information or use *CompanyX* infrastructure.
- Should you decide to sell, recycle, give, or change your device, you will inform the IT Service Desk by phone or email.
- The policy will require a four-digit pin to access your device. Your device or application will lock every 5 minutes requiring re-entry of your pin.
- To access your Outlook e-mail, calendar, and Lync, you will need to enter your network account password. This rotates every 90 days, as per domain policy.
- Backing up your personal files and in the case of a device shared with family or friends, their personal files to your own personal laptop.
- All external email transfers of sensitive information must be a password protected zip file for RESTRICTED. If this cannot be done, then you should not be sending the information on that device.
- You must ensure that your device is compliant, and that security software is kept up-to-date.
- You are responsible for the safekeeping of your own personal data.
- In addition to the above security settings, all users are expected to use their device in an ethical manner. Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, “jailbreaking” your iPhone or “rooting” your android device.

CompanyX Responsibilities

As the data controller, *CompanyX* is responsible for ensuring that all processing for personal data which is under his control remains in compliance with the Data Protection Act 1998.

CompanyX must also remain mindful of the personal usage of such devices and the privacy of the individual. Technical and organisational measures used to protect company owned data must remain proportionate to the risks. A risk-based decision will look at both the risks and opportunities as part of the decision process.

The following will need to be assessed by *CompanyX*:

- What type of data is held
- Where data may be stored
- How it is transferred

- Potential for data leakage
- Blurring of personal and business use
- The device's security capacities
- What to do if the person who owns the device leaves their employment; and
- How to deal with the loss, theft, failure, and support of a device.

Security Incidents

A number of security incidents could occur when using personal devices with *CompanyX* data.

These include:

- Theft or loss of data or any equipment
- Transfer/disclosure of sensitive data to those who are not entitled to receive it
- Compromised passwords
- Attempt (either failed or successful) to gain unauthorised access to data or systems
- Connection of equipment that has either not been approved by *CompanyX* Consulting
- Non-compliance with CompanyX Consulting's information security policies and associated procedures including this policy
- Hacking attempts, virus attacks, phishing etc
- Device "jailbreaking," "rooting," or the equivalent
- Making any other modifications to device hardware and/or OS software beyond routine installation of updates as directly provided by the applicable device maker or mobile operator.
- Performing such actions or making such unauthorised modifications is essentially an "inside attack" on device, application, and data security, and should be treated very seriously.

If a Security Incident should Occur

If a security incident should occur, e.g., your device is lost or stolen or is infected with malware, you are required to inform the IT Service Desk immediately with details.

If You Leave the Employment of *CompanyX* or Your Contract Ends

As part of the leaver's process, your access to *CompanyX* infrastructure and applications will cease and all access to Company data is ceased.

Consequences for Misuse/Disruption

Breach of this policy by a *CompanyX* employee or contractor may lead to disciplinary action, which could result in dismissal, suspension, or termination of your access to the Service and/or prosecution and/or *CompanyX* co-operating with law enforcement organisations, government agencies, other legal authorities or third parties involved in the investigation of any suspected or alleged criminal or civil offence.

Guidelines for Acceptable Behaviour

Device owners are expected to behave in accordance with *CompanyX* behaviours framework at all times whilst undertaking work for the Company. Further information can be obtained your manager or by contacting an HR advisor.

Be aware that any personal device used at work may be subject to discovery in litigation. This means that it could be used as evidence in a lawsuit against *CompanyX*. Your data could be examined not only by *CompanyX* but also by other parties in any lawsuit. A further consideration is that if you travel internationally your device might be subject to search and seizure at border control.

CompanyX Consulting Release of Liability and Disclaimer Statement

CompanyX hereby acknowledges that the use of a personal device in connection with *CompanyX* business carries specific risks for which you, as the device owner and user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data because of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

CompanyX hereby disclaims liability for the loss of any such data and/or for service interruptions. *CompanyX* expressly reserves the right to wipe the device management application (or similar applications) at any time as deemed necessary for the purposes of protecting or maintaining *CompanyX* infrastructure and services.

CompanyX also disclaims liability for device owner injuries such as repetitive stress injuries developed. *CompanyX* provides IT equipment that is suitable for long-term office use.

Device owners bring their devices to use at *CompanyX* as their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

CompanyX is in no way responsible for:

- Personal devices that are broken while at work or during work-sponsored activities
- Personal devices that are lost or stolen at work or whilst undertaking work-related activities
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues)
- The management or creation of users own ‘cloud’ based user accounts, which are required for purchasing software, or backing up data

CompanyX does not guarantee that Service will be compatible with your equipment or warrant that the Service will be always available, uninterrupted, error-free, or free of viruses or other harmful components, although it shall take reasonable steps to provide the best service it can.

Furthermore, depending on the applicable data plan, the software may increase applicable rates. You are responsible for confirming any impact on rates because of the use of *CompanyX* supplied applications as you will not be reimbursed by *CompanyX*.

Finally, *CompanyX* reserves the right, at its own discretion, to remove any *CompanyX* supplied applications from your personal device as a result of an actual or deemed violation of the *CompanyX’s* BYOD Policy.