BRING YOUR OWN DEVICE (BYOD) POLICY

Introduction

The purpose of this document is intended to address the use in the establishment by users (including but not limited to Employee, Students, Visitors, Contractors) of non- establishment owned electronic devices such as smart phones, tablets and other such devices to access and store establishment information, as well as their own. This is commonly known as 'bring your own device' or BYOD.

It is the policy of the establishment to place as few technical restrictions as possible on the development and use of new applications and services. However the use of non-establishment owned devices to process information and data creates issues that need to be addressed particularly in the area of data security.

As data controller the establishment must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing.
IT and Central Services reserves the right to refuse or allow access to a particular device or software where it considers that there is a security or other risk to its systems and infrastructure.

Note for Staff
As an employee you are required to keep secure establishment information and data. This applies equally to information held on the establishment systems and to information held on an employee's own device. As an employee you are required to assist and support he establishment in carrying out its legal and operational obligations with regards to establishment data and information stored on your device. You are required to co-operate with IT Services when they consider it necessary to access or inspect establishment data stored on your device.

1. Security of Systems and Technical Infrastructure

The establishment takes security very seriously and invests significant resources to protect data and information in its care. The establishment is contractually required to comply with the Janet Security Policy, to protect the security of Janet and of its own internal networks.

To this end BYOD has been limited to only allow access to Internet and other web-based technologies (such as E-Mail and other online portals). Access to file shares (such as network drives) are not permitted and controls are in place to prevent it.

Users may access files using Office 365.

Where an employee has been given a device by the establishment to aid them in their work, you are expected to play your part in maintaining the security of data and information that you handle. This includes security of transfer of data between the personal device and the establishment system.

Where an employee uses their own device to access and store data that relates to the Establishment (such as their home computer/laptop/tablet) then it is their responsibility to familiarise themselves with the device sufficiently in order to keep the data secure. In practice this means –

- preventing theft and loss of data
- where appropriate keep information confidential and maintaining the integrity of data and information
- delete sensitive or business information once you have finished with them

- delete copies of attachments to emails such as spread sheets and data sets on mobile devices as soon as you have finished with them
- limit the number of emails and other information that you are syncing to your device

In event of loss or theft of a device you should report the matter promptly to IT Services to enable access to establishment systems by a device or user to be revoked and/or the activation of a remote locate and wipe facility operated by the establishment. It is recognised that remote wiping of data may result in the loss of the employee's personal information held on the device.

Remote locate and wipe will be used at the discretion of IT Services including where there is a risk that confidential data or personal data has been stored on a device that has been lost, stolen or misplaced.

Certain data should never be stored on a personal device. Any establishment data that is kept must be stored with the appropriate level of security and in accordance with the Establishment IT Security/Data Protection policy. If you are in any doubt as to the level of security that should attach to particular data then you are required to consult with your manager or IT Services in order to clarify what protection is appropriate.
Failure to comply with this code is considered a disciplinary offence.

2. Security and e-Safety of Users

The establishment is committed to providing a safe environment for learners and staff including the online environment. Your attention is drawn to the separate Establishment e-safety guidelines that identifies the role that the establishment plays in maintaining a safe online working environment.

As a user you are required to play your part in maintaining a safe working environment and in terms of BYOD this means keeping software up to date and avoiding content that threatens the integrity and security of your device, the establishment systems and the devices of learners and others. It also means ensuring that the device automatically locks if inactive for a period of time.

The establishment Social Media Guidelines applies to the BYOD context. This provides standards expected on appropriate online behaviour including between staff and learners. It is particularly important to maintain a distinction between personal content and work related content especially where interaction that takes place between individuals and where images and content are shared and published.

3. Monitoring of User Owned Devices

The establishment will not monitor the content of user owned devices for threats to the technical infrastructure of the institution. Your attention is drawn to the ICT Acceptable Use Policy which regulates the monitoring of devices used by users for work purposes. IT Services reserves the right to prevent access to the establishment network by any device that is considered a risk to the network.

In exceptional circumstances the establishment will require to access establishment data and information stored on your personal device. In those circumstances every effort will be made to ensure that the establishment does not access the private information of the individual. Establishment data and information can only be stored and processed on personally owned devices under acceptance of these conditions.

If certain secure or confidential categories of data and information are required to be accessed or stored on your own device then the Establishment would be obliged to monitor the device at a level that may harm your privacy and that of anyone you lend your device to. You should

consult with IT Services when secure or confidential categories of data are to be handled in this way.

4. Compliance with Data Protection Obligations (Staff)

The establishment is committed, as data controller, to treating all personal data fairly and lawfully in line with the Data Protection Act 1998 (DPA). This includes the requirement to keep personal data up-to-date, and to handle it securely and to keep it for no longer than is necessary.

As an employee you are required to comply with the establishment data protection policy and requirements.

Your personal responsibility is expected to align with these establishment obligations.

Your attention is drawn to the separate Data Protection Policy which requires you as an individual to process data in compliance with all aspects of the Data Protection Act and this applies equally to processing of data which takes place in the context of BYOD.

As an employee you are also required to assist the establishment in complying with subject access and FOI requests for information and you may be required to search your device and to provide the information requested to the establishment.

5. Acceptable Use of User Owned Devices

The establishment requires that users conduct their online activities which concern the establishment appropriately and in particular in compliance with the terms of the ICT Acceptable Use Policy.

This requirement transcends whatever communications technology or device is being used. Our ICT

Acceptable Use Policy provides guidance on appropriate use of information technology and requires accountability of behaviour by users.

Failure to comply with the ICT Acceptable Use Policy is considered a disciplinary matter.

6. Support

The establishment will endeavour to support all devices however this may not always be possible and IT Services should be consulted to determine usage and compatibility levels.

7. Incidents and Response

Where a security incident, involving a user using their own devices, arises at the establishment this matter will be dealt with very seriously. The establishment will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

IT Services will review what has happened and decide on the most appropriate and proportionate course of action.

Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the establishment ICT Acceptable Use Policy.

Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

This policy has been adopted by Churchward School:

Signed …….. Headteacher

Signed …….. Chair of Governors

Date ……..