Bring Your Own Device (BYOD) Policy 2023

The Purpose of this Document: This document describes acceptable use pertaining to using your own device whilst accessing the Trust systems, services and data.

Created by: Olan Adeyemi

Date agreed by Finance, Resources, Audit and Risk Committee: December 2023

Frequency of Review: Annually

Date of Next Review: March 2024 or earlier in response to statutory changes

Contents

1. Executive Summary

This policy defines acceptable use by The Futures Trust users whilst using “their own” devices, systems and applications, for accessing, viewing, modifying and deleting of Trust held data and accessing its systems.

2. Intended Audience

This policy document applies to:

• All Users accessing The Futures Trust systems, services and data

• Any auditor, internal or external, appointed to review the process

3. Assumptions and Constraints

The Futures Trust is a registered data controller, for the data protection regulations. It is assumed that all staff have an awareness of the importance of data protection and the consequences of the loss of Trust owned personal data, as GDPR / data protection training is mandatory.

4. Related documents

The Policy is linked to the School’s Code of Conduct, Safeguarding and Child Protection, E-Safety, Disciplinary, Data Protection, Data Handling and FOI, Anti Bullying and Dignity at Work, ICT Acceptable Use, Information Security, Reference and Whistleblowing policies.

The copies of which are available from the school’s HR Office. Alternatively, you can download these from the policies section of the school’s HR Support Portal on SharePoint.

5. Definitions

5.1 BYOD / Bring Your Own Device

BYOD / ‘Bring Your Own Device’ refers to Users using their own device or systems (which are not owned or provided to you by the Trust) or applications, to access and store Trust information, whether at the place of work or remotely, typically connecting to the Trust’s Wireless Service or Remote Access Connection.

5.2 Data Controller

The Data Controller is a person, group or organisation (in this case the Trust) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

5.3 User

A member of staff, contractor, visitor, or another person authorised to access and use the Trust’s systems.

6. Policy

6.1 Introduction

This policy covers the use of non-Trust owned/issued electronic devices which could be used to access corporate systems and store Trust information, alongside their own data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

If you wish to BYOD to access Trust systems, data and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the IT Helpdesk. It is the Trust's intention to place as few technical and policy restrictions as possible on BYOD subject to the Trust meeting its legal and duty of care obligations.

The Trust, as the Data Controller, remains in control of the data regardless of the ownership of the device. As a User you are required to keep Trust information and data securely. This applies to information held on your own device, as well as on Trust systems. You are required to assist and support the Trust in carrying out its legal and operational obligations, including co-operating with IT Services or the Data Protection Officer (DPO) should it be necessary to access or inspect Trust data stored on your personal device. The Trust reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that they are unacceptable in terms of security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

7. Advice and Guidance

Advice and guidance on all aspects of this Policy are available via the IT Service Desk or by contacting the Trust ICT Director.

8. System, Device and Information Security

The Trust takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care. The use of your own device MUST adhere to the IT User Policies, namely the ICT Acceptable Use policy, Information Security Policy and Bring Your Own Device (BYOD) Policy.

When you use your own device as a work tool, you MUST maintain the security of the Trust's information you handle (which includes but is not limited to viewing, accessing, storing, sharing, deleting or otherwise processing).

It is your responsibility to familiarise yourself with the device sufficiently to keep data secure.

In practice this means:

• Preventing theft and loss of data (using Biometric/PIN/Password/Passphrase lock)

• Keeping information confidential, where appropriate.

• Maintaining the integrity of data and information.

8.1 You MUST:

- Use the device's security features, such as a Biometric, PIN, Password/Passphrase and automatic lock to help protect the device when not in use.

- Keep the device software up to date, for example using Windows Update or Software Update services.

- Activate and use encryption services and anti-virus protection if your device features such services.

- Install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature. This is to enable you to locate or wipe your device should it go missing.

- Remove any Trust information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets as soon as you have finished using them.

- Remove all Trust information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

8.2 You MUST NEVER:

- Retain personal data from Trust systems on your own device. During the process of receiving a password protected attachment, the file may automatically store on your device. This file should be deleted as soon as it has been used or if it needs to be kept, save this within your allocated OneDrive.

- If you are in any doubt as to whether particular data can be stored on your device you are required to err on the side of caution and consult with your manager, or seek advice from the IT Helpdesk.

- Personal data as defined by the data protection laws may not be stored on personal cloud services. You should use the Trust provided storage such as OneDrive.

9. The loss, theft or security compromise of a device

9.1 In the event that your device is lost or stolen, or its security is compromised, you MUST promptly report this to the IT Helpdesk, in order that they can assist you to change the password to all Trust services (it is also recommended that you do this for any other services that have accessed via that device, e.g. social networking sites, online banks, online shops).

9.2 In the event that it is necessary to do so, you must also cooperate with Trust ICT Director in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.

9.3 You MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example to 'jailbreak' the device.

9.4 Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the IT Helpdesk.

10. Monitoring of User Owned Devices

10.1 The Trust will not monitor the content of your personal devices; however, the Trust reserves the right to monitor and log data traffic transferred between your device and Trust systems, both over internal networks and entering the Trust via the Internet.

10.2 In exceptional circumstances, for instance where the only copy of a Trust document resides on a personal device, or where the Trust requires access in order to comply with its legal obligations (e.g. under the GDPR / Data Protection Act, the Freedom of Information Act, or where obliged to do so by a Court of law or other law enforcement authority) the Trust will require access to Trust data and information stored on your personal device. Under these circumstances all reasonable efforts will be made to ensure that the Trust does not access your private information.

10.3 You are required to conduct work-related, online activities in line with the Trust's Computer Use Regulations. This requirement applies equally to using devices of your own used for work purposes.

11. Responsibilities regarding Device Support

11.1 Where possible the Trust supports all devices, but you have a responsibility to learn how to use and manage your device effectively in the context of this policy. Help and advice is available on a reasonable endeavours basis, via the IT Helpdesk.

11.2 The Trust takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

11.3 You can access the Trust's BYOD Guidance on how to protect your computer from the policies section of the school's HR Support Portal on SharePoint.

12. Appendix A

BYOD Acceptable Use Agreement

I have read and understood the above BYOD policy. I understand that I must use the security features on my device to protect access. I must also keep the device software up to date. I understand that I must never retain personal data from Trust systems on my own device. And that I will promptly report any loss, theft or compromise of the device to the IT helpdesk.

I understand it is my responsibility to learn how to use and manage my device effectively in the context of this policy.

Job Title / Position	
Staff / Volunteer Name	
Signed	
Date	

If you are uncertain regarding any aspects of the BYOD Policy and have any questions, you must ask for clarification from the School's ICT Department before signing this declaration.