PDET

Bring Your Own Device (BYOD) Policy

Date	Revision & Amendment Details	By Whom
January 2023	Reviewed and approved	Central Executive Team

Guidance

The Trust’s Acceptable Use Policy (AUP) does not permit the use of personal devices for Trust work and/or to access Trust data. However, in limited circumstances, specific written permission may be given.

One such circumstance is in relation to teaching assistants in the Trust who do not have access to a Trust laptop/tablet and need to use their own personal device for Trust/school work purposes.

In addition, as we further the deployment of Microsoft Office 365 there will be a number of security measures being implemented to better protect users, devices, and data. As part of this it may become necessary to support the use of personal mobile devices for user authentication (e.g. for sending one-time passcodes via text, or obtaining access codes via the MS Authenticator app), and also the ability to use a secure Trust-provided series of MS Office apps on mobile devices (whether issued by the Trust or personally owned devices).

If specific written permission is given in accordance with this policy, it must be documented as per the form in Appendix 1 and use of such personal devices must be in accordance with:

- the terms of this policy;
- the AUP; and
- the Trust’s Clarification and Guidance in Relation to the AUP.

In Appendix 2 is a form that the Trust/schools can use to record actions

Bring Your Own Device Policy

Our Vision

Peterborough Diocese Education Trust and all the schools within it (the Trust) embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. The Trust is also aware:

- that inappropriate, or misguided use, can expose both adults and children to unacceptable risks and dangers; and
- of the need to protect the integrity of the Trust's data and ensure it remains safe and secure under the Trust's control.

To that end, the Trust has put in place its:

- Acceptable Use Policy (AUP);
- Clarification and Guidance in relation to the AUP;
- Remote Education: Guidelines for Parents / Carers and Pupils
- Remote Education: Online Safety (Safeguarding and GDPR Considerations) Guidance for Schools / Academies.

in addition to its Policy and Procedures on Safeguarding and Child Protection.

Scope

The AUP does not permit Trust employees or those undertaking work for the Trust (referred to in this policy as 'users') to use their own personal devices (referred to as 'Device(s)' in this policy) including, but not limited to, laptops, computers, smartphones and tablets to access the Trust's (which includes schools') networks, or undertake work for the Trust, without permission from their Headteacher/Manager.

The Trust recognises that, in certain limited circumstances, it is appropriate for permission to be granted and this policy sets out the criteria/conditions that must apply in relation to use of a personal Device if permission is granted.

The Trust's data remains the property of the Trust at all times no matter what format it is in, where it is stored, or how it is accessed, and the Trust remains responsible for the retention of its data.

Criteria and conditions for use of Devices

General

If permission is granted pursuant to the AUP:

- for the use of personal devices in relation to security, authentication, or app access to the Trust-provided Microsoft 365 services, no further documentation or approval is required;
- for any and all other uses of personal devices these must be documented on the form attached at Appendix A; and

- under either of these situations users agree to use the Device in accordance with the AUP, the AUP Clarification and Guidance Document and the following general code of conduct/usage, which recognises the need to protect data, in particular confidential data, that is stored on, or accessed using, a Device.

This **code of conduct/usage** includes but is not limited to:

Ensuring the Device is kept secure:

- A strong password (the National Cyber Security Centre advise using 3 random words) or a PIN must be used to lock the Device, to prevent others from accessing data through it;
- Devices must be immediately locked when leaving them unattended;
- Access to Trust data via Devices must not be shared with family or friends;
- Security software must be installed;
- Antivirus software must be installed on laptops and computers and kept up to date with regular scans taking place, e.g. McAfee;
- Operating systems and any installed applications must be kept up to date;
- Devices must not be used in ways not designed or intended by the manufacturer and the user must ensure that the Device's security controls are not subverted via hacks, jailbreaks, 'rooting', security software changes and/or security setting changes.

Not storing Trust data or access to it on Devices:

- All data relating to the Trust must be stored on the Trust network (including approved cloud based storage systems). Under no circumstances should Trust data be saved directly to Devices;
- Any temporary downloads to Devices must be securely deleted immediately after use;
- Passwords used to access Trust data must not be saved to Devices or within password management systems.

Deletion of/access to data

- When permission to use Devices is removed and/or at the point of ceasing working for/undertaking work for the Trust, written confirmation of secure deletion of all Trust data must be given to the Headteacher/Manager.
- Users agree to give the Trust access to any Trust owned data on Devices immediately upon the reasonable request of the Trust. 'Access' includes being permitted to access, make copies of, recover or delete files containing Trust owned information from Devices;
- Any loss, theft, compromise or data security breach, or suspected breach, must be reported immediately (see below).

Responsibility and liability

Whilst Devices can be connected to the Trust's network, users are personally liable for

Devices and carrier service costs and any related costs such as security, anti-virus software, repairs and insurance. The User is also responsible for:

- Settling any service or billing disputes with the carrier;
- Purchasing any required software not provided by the manufacturer or wireless carrier;
- Device registration with the vendor and/or service provider;
- Maintaining any necessary warranty information;
- Battery replacement due to failure or loss of ability to hold a charge;
- Installation of software updates/patches;
- Any support need or issue.

Security requirements

The user is responsible for securing Devices to prevent data from being lost or compromised and to prevent viruses from being spread. When undertaking Trust/school work, the removal of security controls is prohibited.

Users are forbidden from copying data from the Trust/school's network, email, calendar and contact applications to other applications on the Device or to an unapproved Device. This also includes moving data to other insecure storage areas such as personally-owned USB sticks and external hard drives.

Loss, theft, compromise and data security breaches

If the Device is lost or stolen, is believed to have been compromised in some way, or there is a data security breach, the user must report the incident immediately to the Trust's DPO (dpo @pdet.org.uk) and to the Headteacher/Manager.

Enforcement

Any user found to have breached this policy may be subject to disciplinary action, including but not limited to:

- Account suspension;
- Revocation of permission to use the Device for Trust work/access to the Trust's network;
- Data removal from the Device;
- Employee Termination.

Other provisions

- The Trust must ensure that a user's account will be locked after 3 failed login attempts.
- The Trust reserves the right to access Devices used for Trust work/purposes for audit purposes.
- The Trust reserves the right to disable or disconnect some or all services without prior notification.

Disclaimer

The Trust hereby acknowledge that the use of a personal Device in connection with Trust business carries specific risks for which the user, assumes full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the operating system, errors, bugs, viruses, downloaded malware, and/or other software or hardware failures, or programming errors which could render a Device inoperable.

Appendix 1

Request for permission to use a personal device

Name ____

Type of device to be used (e.g. mobile phone, laptop):

Why do you need to use your personal device for Trust/school work and/or to access Trust/school data?

If temporary access needed - date of access needed and timescale

Confirmation:

I have read and accept the terms and conditions contained within the Bring Your Own Device Policy, Acceptable User Policy and AUP Clarification and Guidance Document.

Signed………………………………………………………………………………..Date…………………………………….

To be completed by Headteacher / Manager

Date permission given	
Date for review	
Signature	

Appendix 2

Template record to be kept by Trust/school

Name of user	Confirmation of receipt of acceptance of BYOD and AUP (including clarification and guidance document) terms and conditions (yes / no)	Date permission given	Review date	Date access removed	Confirmation from user of deletion of data