DDAT

Derby Diocesan Academy Trust

Bring Your Own Device Policy (BYOD)

March 2025

Approved by the Trust Board on: 18th March 2025

Due for Review on: March 2026

Contents

1 Introduction 2
2 Scope and Responsibilities 3
3 Use of mobile devices at school 3
4 Access to the school's Internet connection 4
5 Access to School IT systems 4
6 Monitoring the use of mobile devices 4
7 Security of staff personal devices 5
8 Permissible and non-permissible use 5
9 Use of cameras and recording equipment 6

1 Introduction

As a Trust and across our schools, we recognise that mobile technology offers valuable benefits to staff and students from a teaching and learning perspective and to visitors. The Trust and its schools embrace this technology but requires that it is used in an acceptable and responsible way. The Trust/School will not compel staff to use their own personal devices to access Trust/school systems, but if staff choose to use their own devices, this policy should be adhered to.

Guest devices (any device which is not Trust/school owned or on the Trust/school asset list) should only be connected to a secure segregated network for access.

This policy is designed to support the use of guest devices (any device which is not Trust or school owned or on the Trust or school asset list) in the Trust or its schools in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the Trust and school networks and explain what constitutes acceptable use and misuse of the BYOD policy.

This policy supports our Data Protection Policy and provides guidance on how to minimise risks associated with the use of guest devices, in line with the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

The purpose of this policy is to preserve the security and integrity of Trust and school data and systems. It does not expressly or by implication provide permission to use any non-Trust or non-school device. Rather, it sets out the organisational and technical measures in place where such permission is granted in the staff and visitors code of conduct, pupil behaviour policy and social media policy. It has been reviewed in light of the publishing of the Mobile phones in schools – February 2024 (publishing.service.gov.uk)

The Trust and its Schools reserves the right to refuse staff and visitors permission to use their personal devices on school premises.

This applies to all guest devices connecting to Trust or school systems.

Personal external hard drives and memory devices/USB sticks are not permitted and should not be inserted into school/Trust devices.

This policy should be read in conjunction with the Trust Central Team HR advice and guidance and associated policies and procedures.

2 Scope and Responsibilities

This policy applies to all use of guest devices to access the internet via the Trust or its school's guest network or to access Trust or school information, by staff, pupils or visitors. This is known as “Bring Your Own Device”, or “BYOD”. Guest devices include laptops, tablets, smart phones, USB sticks, wearable technology (including smart / apple watches) and any other device considered portable and/or with the ability to connect to WiFi and the Internet which is not Trust or school owned or on the Trust or school asset list, including staff personal devices.

All staff and other users are responsible for reading, understanding and complying with this policy if they are using their personal devices connected to the school Internet, or using personal devices to access information held on Trust or school systems.

If you have any concerns surrounding the use of personal devices, please contact the Executive Headteacher/ Headteacher or Designated Safeguarding Lead in schools or the COO for the Central Team.

Users should be aware of the need to;
- Protect children from harm
- Understand what constitutes misuse
- Minimise risk from BYOD
- Report suspected misuse immediately
- Be responsible for their own professional behaviour
- Respect professional boundaries

3 Use of mobile devices at the Trust or its schools

Permission must be sought before connecting personal devices to the Trust or school’s network. The Trust and its school’s reserve the right to refuse staff, pupils and visitors permission to use their personal devices on Trust or school premises.

Staff, pupils and visitors are responsible for their personal devices at all times. The Trust and its schools are not responsible for the loss, or theft of, or damage to the personal device or storage media on that device (e.g. removable memory card) howsoever caused, including lost or corrupted data.

The Trust or the relevant school must be notified as soon as possible of any loss, or theft of a personal device that has been used to access Trust or school systems, and these incidents will be logged with the DPO. Please also log via GDPRiS.

Data protection incidents should be reported immediately to the Trust’s Data Protection Officer/COO.

Personal devices used to access Trust or school systems must enable automatic updates for security patches from the supplier. Applications installed on the device must also be subject to regular security updates, be supported by the supplier and licensed.

The Trust and its schools cannot support users’ personal devices, nor has the Trust or school a responsibility for conducting annual PAT testing of personal devices.

4 Access to the Trust or its school's Internet connection

The Trust and its schools provide a guest network connection that staff, pupils and visitors may, with permission, use to connect their personal devices to the Internet under exceptional circumstances. Access to the network is at the discretion of the Trust or school, and they may withdraw access from anyone it considers is using the network inappropriately.

The Trust and its schools cannot guarantee that the wireless network is secure, and staff, pupils and visitors use it at their own risk. In particular, staff, pupils and visitors are advised not to use the wireless network for online financial transactions.

The Trust and its schools do not permit the downloading of apps or other software whilst connected to the Trust or school network and they are not responsible for the content of any downloads onto the user's own device whilst using the Trust or its school's network.

The Trust and its schools accept no liability for any loss of data or damage to personal devices resulting from use of the Trust or its school's network.

5 Access to Trust or School IT systems

Where staff are permitted to connect to Trust or school IT systems from their personal devices, a second layer of security should be enabled such as a password and/or encryption/MFA and notifications must be turned off the lock screen. It is the responsibility of the owner of that device to ensure it is safe for the purposes for which they wish to use it.

Staff must **not** store personal data about pupils or others on any personal devices, or on cloud servers linked to their personal accounts or devices.

With permission, it may be necessary for staff to download Trust or school information to their personal devices in order to view it (for example, to view an email attachment). Email attachments are the most common source of cyber-attacks. Please follow staff guidance on cyber security and email protection and be aware that personal devices are not subject to the same security controls and safeguards that protect the Trust and its school's network and devices.

Any unauthorised access to, or distribution of, confidential information should be reported to the Data Protection Officer/COO/Executive Headteacher/Headteacher and logged via GDPRiS as soon as possible in line with the Trust and school's data protection policies. This includes theft or loss of a personal device which has been used to connect to Trust or school information systems, or which may contain personal data.

Before selling or giving your personal device which has been used to access the Trust or school network including cloud-based systems to someone else, including a family member or spouse, it must be cleansed of all Trust or school related data, emails, systems and apps.

6 Monitoring the use of mobile devices

The Trust and its school's reserve the right to use technology that detects and monitors the use of personal devices, which are connected to or logged on to our network or IT systems. The use of such technology is for the purpose of ensuring the security of its IT systems and Trust or school information.

The information that the Trust and its schools may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded to or downloaded from websites and Trust or school IT

systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Any inappropriate content received through the Trust or school IT services or the Trust or school's internet connection should be reported to the COO/ Executive Headteacher/Headteacher / IT Lead / Designated Safeguarding Lead as soon as possible.

7 Security of staff personal devices

Staff must take all sensible measures to prevent unauthorised access to their personal devices, including but not limited to the use of a PIN, pattern or password to unlock the device, and ensuring that the device auto-locks if inactive for a short period of time.

The Trust and its school's Acceptable Use of IT and IT Security policies set out in further detail the measures to ensure responsible behaviour online.

8 Permissible and non-permissible use

Staff and visitors participating in BYOD must comply with the ICT Acceptable Use Policy.

- Where there are particular safeguarding or safety requirements in some settings, the Executive Headteacher/Headteacher has the right to require storage of staff or visitor devices in a secure location such as staff lockers or similar secure location.
- The Executive Headteacher/Headteacher can decide if devices can or cannot be taken into areas around the Trust or school premises where there are particular safeguarding issues (such as changing rooms). In such cases, the Trust or school should agree with and inform staff, pupils and visitors the areas which are expected to be "BYOD free".
- Visitors and contractors to the Trust or its school sites should be informed of the policy regarding personal devices upon arrival (please also refer to the DDAT Staff and Visitors Code of Conduct).
- Personal devices must not be taken into controlled assessments and/or examinations, unless special circumstances apply.
- Staff, volunteers and contractors should not use their own personal mobile phone for contacting children and young people or parents/ carers, unless it is an emergency, and they are unable to use or access the school's telecommunication systems. If this occurs, their telephone number should be withheld.
- If it is necessary for a phone call or text to be taken or received, care should be taken to avoid disturbance or disorder to the running of the Trust or school.

9 Use of cameras and audio recording equipment

Visitors and staff subject to this policy may not use their own mobile devices to take photographs, video, or audio recordings in school. Recordings in these circumstances will be carried out in line with our Data Protection and HR policies and procedures.

Photographs, video or audio recordings that are taken using Trust/school devices and are to be retained for further legitimate use, they should be stored securely via the Trust or its School's network. The Trust and its school's ensures it is compliant in relation to KCSIE.

In order to protect the privacy of our staff and pupils, and, in some cases their safety and wellbeing, photographs, video, or audio recordings must not be published on blogs, social networking sites or disseminated in any other way without the permission of the people identifiable in them.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school (for further information, please refer to the DDAT Social Media Policy).