



Tudor Grange Academies Trust

Bring Your Own Device Policy (BYOD)

Document title	Bring Your Own Device Policy (BYOD)
Author/originator	S Groutage / Education Data Hub
Date of Approval	16 April 2026
Approving Committee	Operations Committee
Version	1.0
Policy review date	Annual – April 2027

Date updated	Version	Change from last version
16.04.2026	1.0	New policy

Contents

1. Introduction.....	2
2. Scope and Responsibilities	3
3. Use of mobile devices at the Trust.....	3
4. Access to the Trust’s Internet connection	4
5. Access to Trust 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 audio recording equipment.....	5

1. Introduction

- 1.1. We recognise that mobile technology offers valuable benefits to staff and students from a teaching and learning perspective and to visitors. Our Trust (Tudor Grange Academies Trust, “the Trust”) embraces this technology but requires that it is used in an acceptable and responsible way. The Trust will not compel Trust staff to use their own personal devices to access Trust systems, but if staff choose to use their own devices, this policy will be adhered to.
- 1.2. Guest devices (any device which is not Trust owned or on the Trust asset list) will only be connected to a secure segregated network for access. The DfE digital and technology standards in schools and colleges advise that schools/colleges should have implemented NACs (network access controls) and Policy Management that ensures authorised mobile user devices or guest user roles are securely authenticated onto the network. Switches are configured to support network segregation, security and quality of service. This can be found in the [Wireless network standards for schools and colleges](#) and [Network switching standards for schools and colleges](#).
- 1.3. This policy is designed to support the use of guest devices (any device which is not Trust owned or on the Trust asset list) in the Trust in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the Trust networks and explain what constitutes acceptable use and misuse of the BYOD policy.
- 1.4. 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).
- 1.5. This applies to all guest devices connecting to Trust systems.
- 1.6. The purpose of this policy is to preserve the security and integrity of Trust data and systems. It does not expressly or by implication provide permission to use any non-Trust device. Rather, it sets out the organisational and technical measures in place where such permission is granted in the adult code of conduct and behaviour policy. It has been reviewed in light of the [Mobile phones in schools - February 2024 \(publishing.service.gov.uk\)](#)

- 1.7. The Trust reserves the right to refuse staff, pupils and visitors permission to use their personal devices on Trust premises.
- 1.8. This policy will be read in conjunction with the Trust HR advice and guidance and the Online Safety Policy.

2. Scope and Responsibilities

- 2.1. This policy applies to all use of guest devices to access the internet via the Trust's guest network or to access Trust 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 Wi-Fi and the Internet which is not Trust owned or on the Trust asset list, including staff personal devices.
- 2.2. 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 Trust Internet, or using personal devices to access information held on Trust systems.
- 2.3. If you have any concerns surrounding the use of personal devices, please contact our Principal or Designated Safeguarding Lead.
- 2.4. Users will be aware of the need to;
 - Protect children from harm
 - Understand what constitutes misuse
 - Minimise risk from BYOD
 - Protect the organisation from cyber incident
 - Report suspected misuse immediately
 - Be responsible for their own professional behaviour
 - Respect professional boundaries

3. Use of mobile devices at the Trust

- 3.1. Permission will be sought before connecting personal devices to the Trust's network. The Trust reserves the right to refuse staff, pupils and visitors permission to use their personal devices on Trust premises.
- 3.2. Staff, pupils and visitors are responsible for their personal devices at all times. The Trust is 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.
- 3.3. The Trust will be notified as soon as possible of any loss, or theft of a personal device that has been used to access Trust systems, and these incidents will be logged with the DPO.
- 3.4. Data protection incidents will be reported immediately to the Trust's Data Protection Officer.
- 3.5. Personal devices used to access Trust systems will enable automatic updates for security patches from the supplier. Applications installed on the device will also be subject to regular security updates, be supported by the supplier and licensed.
- 3.6. Where applicable, anti-virus and anti-malware software will be installed onto any device intended to access Trust systems.
- 3.7. The Trust cannot support users' personal devices, nor has the Trust a responsibility for conducting annual PAT testing of personal devices.

4. Access to the Trust's Internet connection

- 4.1. The Trust provides a network connection that staff, pupils and visitors may, with permission, use to connect their personal devices to the Internet. Access to the network is at the discretion of the Trust, and the Trust may withdraw access from anyone it considers is using the network inappropriately.
- 4.2. Although the Trust provides secure wireless networks to the schools, it cannot guarantee that devices accessing networks are secure, and staff, pupils and visitors use them at their own risk. In particular, staff, pupils and visitors are advised not to use the wireless network for online financial transactions.
- 4.3. The Trust does not permit the downloading of apps or other software whilst connected to the Trust network and the Trust is not responsible for the content of any downloads onto the user's own device whilst using the Trust's network.
- 4.4. The Trust accepts no liability for any loss of data or damage to personal devices resulting from use of the Trust's network.

5. Access to Trust IT systems

- 5.1. Where staff are permitted to connect to Trust IT systems from their personal devices, a second layer of security should be enabled such as a password and/or encryption and notifications should 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.
- 5.2. Staff will **not** store personal data about pupils or others on any personal devices, or on cloud servers linked to their personal accounts or devices.
- 5.3. With permission, it may be necessary for staff to download Trust 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 network and devices.
- 5.4. Any unauthorised access to, or distribution of, confidential information will be reported to the Principal and Data Protection Officer as soon as possible in line with the Trust's data protection policies. This includes theft or loss of a personal device which has been used to connect to Trust information systems or which may contain personal data.
- 5.5. Before selling or giving your personal device which has been used to access the Trust network including cloud-based systems to someone else, including a family member or spouse, it should be cleansed of all Trust related data, emails, systems and apps.

6. Monitoring the use of mobile devices

- 6.1. The Trust reserves 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 information.
- 6.2. The information that the Trust 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 IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.
- 6.3. Any inappropriate content received through Trust IT services or the Trust internet connection will be reported to the Principal or Designated Safeguarding Lead as soon as possible.

7. Security of staff personal devices

- 7.1. Staff will 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.
- 7.2. The Trust's Acceptable User Agreement (an appendix of the Online Safety Policy) sets out in further detail the measures to ensure responsible behaviour online.

8. Permissible and non-permissible use

- 8.1. Staff and visitors participating in BYOD will comply with the Acceptable User Agreement.
 - Where there are particular safeguarding or safety requirements in some settings, for example, in special schools and nurseries, the Principal has the right to require storage of staff or visitor devices in a secure location such as staff lockers.
 - The Principal can decide if devices can or cannot be taken into areas around the school where there are particular safeguarding issues (such as changing rooms). In such cases, the Trust will agree with and inform staff, pupils and visitors the areas which are expected to be "BYOD free".
 - Visitors and contractors to the Trust site will be informed of this policy regarding personal devices upon arrival.
 - Personal devices will not be taken into controlled assessments and/or examinations, unless special circumstances apply.
 - Staff, volunteers and contractors will 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 Trust's telecommunication systems.
 - If it is necessary for a phone call or text to be taken or received, care will be taken to avoid disturbance or disorder to the running of the Trust.

9. Use of cameras and audio recording equipment

- 9.1. Visitors and staff subject to this policy may not use their own mobile devices to take photographs, video, or audio recordings in the Trust without the explicit permission of the Principal.
- 9.2. Where staff are permitted to use their own mobile device for photographs, then photographs, video or audio recordings made by staff on their own mobile devices must be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the School's social media sites. If photographs, video or audio recordings are to be retained for further legitimate use, they will be stored securely via the Trust network.
- 9.3. In order to protect the privacy of our staff and pupils, and, in some cases their safety and wellbeing, photographs, video, or audio recordings will not be published on blogs, social networking sites or disseminated in any other way without the permission of the people identifiable in them.
- 9.4. No one will use mobile devices to record people at times when they do not expect to be recorded, and devices will not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in the Trust (for further information, please refer to our Social Media Policy).