



BRING OWN DEVICE POLICY

SANDON PRIMARY ACADEMY

Mrs R Beckett & Mrs L Kiddle (Co-Principals)

Contents

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

1. Introduction

- We recognise that mobile technology offers valuable benefits to staff and pupils from a teaching and learning perspective and to visitors. The academy embraces this technology but requires that it is used in an acceptable and responsible way. The academy does not compel school staff or pupils to use their own personal devices to access school systems (as school devices are provided to all), but if staff and pupils choose to use their own devices, this policy should be adhered to.
- Guest devices (any device which is not school owned or on the school asset list) should only be connected to a secure segregated network for access-8612080.11BYOD
- This policy is designed to support the use of guest devices (any device which is not school owned or on the school asset list) in school in a way that extends and enhances teaching and learning. It also aims to protect children from harm, minimise risk to the academy networks and explain what constitutes acceptable use and misuse of the bring your own device 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 academy reserves the right to refuse staff and visitors permission to use their personal devices on school premises.
-

2. Scope and Responsibilities

This policy applies to all use of guest devices to access the internet via the academy's network or to access academy 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 school owned or on the school asset list, including staff personal devices.

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

If you have any concerns surrounding the use of personal devices, please contact our Principal or Designated Safeguarding Lead.

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 academy

Permission must be sought before connecting personal devices to the school's network. The academy reserves the right to refuse staff, pupils and visitors permission to use their personal devices on school premises.

Staff, pupils and visitors are responsible for their personal devices at all times. The academy 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.

The academy must be notified as soon as possible of any loss, or theft of a personal device that has been used to access academy systems, and these incidents will be logged with the Data Protection Officer (Kate Burrows).

Data protection incidents should be reported immediately to the academy's Data Protection Officer.

Personal devices used to access academy 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 academy cannot support users' personal devices, nor has the academy a responsibility for conducting annual PAT testing of personal devices.

4. Access to the academy's Internet connection

The academy 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 academy, and the academy may withdraw access from anyone it considers is using the network inappropriately.

The academy cannot guarantee that the wireless network is fully 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 academy does not permit the downloading of apps or other software whilst connected to the academy network and the academy is not responsible for the content of any downloads onto the user's own device whilst using the academy's network.

The academy accepts no liability for any loss of data or damage to personal devices resulting from use of the academy's network.

5. Access to academy IT systems

Where staff are permitted to connect to academy IT systems from their personal devices, a second layer of security should be enabled such as a password and/or encryption 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 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. Staff must be aware that personal devices are not subject to the same security controls and safeguards that protect the academy network and devices.

Any unauthorised access to, or distribution of, confidential information should be reported to the Principal and Data Protection Officer (Kate Burrows) as soon as possible in line with the academy's data protection policies. This includes theft or loss of a personal device which has been used to connect to academy information systems or which may contain personal data.

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

6. Monitoring the use of mobile devices

The academy 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 academy information.

The information that the academy 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 academy IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Any inappropriate content received through academy IT services or the academy internet connection should be reported to the Principal / 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 academy's Acceptable Use of IT 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.

- The Principal can decide if devices can or cannot be taken to classrooms or other areas around the academy where there are particular safeguarding issues (such as changing rooms). In such cases, the academy will agree with and inform staff, pupils and visitors of the areas which are expected to be "BYOD free".

- Visitors and contractors to the academy should be informed of the policy regarding personal devices upon arrival.
- 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 academy's telecommunication systems.

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 the academy unless permission is granted.

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 inside the academy.

10. Compliance, sanctions and disciplinary matters

Non-compliance of this policy exposes both staff and the academy to risks. If a breach of this policy occurs, the Staff Disciplinary policy will be applied.