The

Lloyd Williamson
Schools Foundation

E-Safety Policy:
Bring Your Own Device (BYOD) Policy for Staff and Visitors

2021-2022

Introduction

The Lloyd Williamson Schools Foundation recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. Our school encourages this technology but requires that it is used in a manner that we deem acceptable and responsible.

This policy is intended to address the use of personal devices by staff members and visitors to the school. These devices include any non-school owned electronic devices. These devices are used for a range of reasons such as to access the Internet via the school's internet connection or to access or store school information.

These devices include (but aren't limited to) smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy please check with the school's IT Lead (Shaun).

These devices are referred to as 'mobile devices' in this policy.

Sections one, two and four of this policy apply to all school staff and to visitors to the school. The rest of the policy is only relevant to school staff. This policy is supported by the school's E-safety Policy.

Policy statements

1. Use of mobile devices at the school

Staff must only use mobile devices in the staff room, during free time, unless as part of a planned lesson. If a mobile device will be used for a planned lesson consent should be obtained from senior management and the reason for its use should be explained to the IT Lead to ensure the safety of staff, students and the overall IT network.

Visitors to the school may use their own mobile devices in the following locations:

- In the staff room or the meeting rooms

- Usually, visitors' mobile devices should be handed in to the front office
- If visitors need to use mobile devices in any part of the school outside of the staff room or meeting room, consent should be obtained by senior management and and the reason for its use should be explained to the IT Lead to ensure the safety of staff, students and the overall IT network.

Staff and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss, or theft of, or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. The office must be notified immediately of any damage, loss, or theft of a
mobile device, and these incidents will be logged in the office incident book.

Mobile devices must be turned off while in the building unless in use in a designated area and/or at a prohibited time (e.g. lunch breaks) and must not be taken into any other areas of the school, unless special circumstances apply (see section 1 Use of mobile devices at the school).

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises.

2. Access to the school's Internet connection

The school provides a wireless network that staff and visitors to the school may use to connect their mobile devices to the Internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for any personal us such as online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

3. Access to school IT services

All School staff are allowed to connect to or access the following school IT services from their mobile devices:

- The school e-mail webmail (where appropriate encryption technologies have been deployed);
- Specific online learning (IXL, REN Learning and GL assessments)

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it. Where personal or sensitive data is used in this way devices or files MUST be encrypted. See IT lead for assistance on encryption. Staff must only use the IT services listed above (and any information accessed through them) for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT Lead and senior management as soon as possible in line with the school's data protection policies.

Staff must not send school information to their personal email accounts.
If in any doubt the user should seek clarification and permission from the school's
IT lead before attempting to gain access to a system for the first time. Users must follow
the written procedures for connecting to the school systems.

4. Monitoring the use of mobile devices

The school uses technology that detects and monitors the use of mobile and other
electronic or communication devices, which are connected to or logged on to our
wireless network or IT systems. By using a mobile device on the school's IT network, staff
and visitors to the school agree to such detection and monitoring. The school's use of such
technology is for the purpose of ensuring the security of its IT systems and for tracking
school information.
The information that the school 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 (including passwords), information uploaded to
or downloaded from websites and school IT systems, the content of emails sent via
the network, and peer-to-peer traffic transmitted via the network.
Staff who receive any inappropriate content through school IT services or the school
internet connection should report this to the school's IT lead as soon as possible.

5. Security of staff mobile devices

Staff must take all sensible measures to prevent unauthorised access to their mobile
devices, including but not limited to the use of a PIN, pattern or password to be
entered to unlock the device, and ensuring that the device auto-locks if inactive for a
period of time. Staff must never attempt to bypass any security controls in school systems
or others' own devices.
Staff are reminded to familiarise themselves with the school's e-safety, Computers and
Internet Access Policy and Media policy which set out in further detail the measures
needed to ensure responsible behaviour online.
Staff must ensure that appropriate security software is installed on their mobile
devices and must keep the software and security settings up-to-date.

6. Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the school's compliance
with the Data Protection laws. Staff must apply this BYOD policy consistently with the
school's Data Protection guidelines.
Where such devices are used to process data of a personal or sensitive nature
appropriate encryption of files or devices must be used. All such data should be
backed up to the school's network or school's Google or Office 365 accounts and

deleted from mobile devices as soon as work has been completed.

7. Support

The school cannot support users' own devices but will offer advice to users in their use where practically possible. The school takes no responsibility for supporting staff's own devices; The school conducts annual PAT test on school devices and equipment. The school holds no responsibility for conducting annual PAT testing of personally-owned devices but we may request staff/ visitors to bring in any equipment or devices that will be used on site. It then becomes the responsibility of each individual to bring in their equipment on the days set out so they can be tested along with school devices.

8. Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs the school may discipline staff in line with the school's disciplinary procedure. Training will also be offered to staff to support them in complying with this policy. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the user in question's permission to use the device on school premises will be withdrawn. For persistent breach of this policy, the school will permanently withdraw permission to use user-owned devices in school.

9. Incidents and Response

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of a mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the school's data protection officer.

Reviewed by: Shaun Watson, IT Lead
Review date: September 2021