# BRING YOUR OWN DEVICE (BYOD) POLICY FOR STAFF (AND VISITORS)

## Introduction

The school recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by staff members and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include 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 Director of Computing. These devices are referred to as 'mobile devices' in this policy.

**Sections one to three and five 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 Staff ICT Acceptable Use Policy.

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually.

## Policy statements

1. Use of mobile devices at the school

Staff and visitors to the school may use their own mobile devices in the following locations:

- In the classroom with the permission of the teacher
- In the school environs – staffroom, School staff accommodation, Headmaster's House (the Facilities Officers and Bursar may use these whilst on site)

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 Bursar must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply. See also the Policy on Photographic Images of Children and the Child Protection Policy ( www.st-andrews.woking.sch.uk/school-policies ) The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises.

## 2. Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own mobile devices to make photographs, video, or audio recordings in school **provided they first obtain permission** to take photographs, films or recordings of the relevant individuals. This includes people who might be identifiable in the background.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them. Parents or carers should avoid commenting on activities involving pupils other than their own in photographs, video, or audio, and other visitors and staff should not comment.

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. Staff must comply with the school's social media policy and anti-bullying policy www.st-andrews.woking.sch.uk/school-policies (and Policy on Photographic Images) when making photographs, videos, or audio recordings.

## 3. 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 online banking or shopping.

Guests access the wireless network via a dedicated system which is remote from the school's network. This is a captive portal system which gives the user eight hours use of the internet using a one-time logon.

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.

## 4. Access to school IT services

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

- the school email system;
- the school MIS;
- the school's cloud services;
- the school's remote desktop services;

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.

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 team or the Bursar as soon as possible.

Staff must not send school information to their personal email accounts.

If in any doubt a device user should seek clarification and permission from the school's IT team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

**5. Monitoring the use of mobile devices**

The school may use 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, 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 team or the Bursar as soon as possible.

**6. 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, social media and acceptable use of IT policies 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.

**7. Compliance with Data Protection Policy**

Staff compliance with this BYOD policy is an important part of the school's compliance with the Data Protection Act 2018. Staff must apply this BYOD policy consistently with the school's Data Protection Policy. www.st-andrews.woking.sch.uk/school-policies

## 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 will respond immediately by issuing a verbal then written warning to the staff member. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily 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 the mobile device should be reported to the Bursar in the first instance. Data protection incidents should be reported immediately to the school's data protection lead, Alastair Law.

| | |
|---|---|
| Compiled by: A Law / M McCue | Policy version date: September 2022 |
| Approved by: SLT | Next Revision date: September 2023 |