GIGGLESWICK SCHOOL

BRING YOUR OWN DEVICE (BYOD – INC MOBILES) POLICY FOR STUDENTS

Introduction

The school recognises that mobile technology offers valuable benefits to students from a teaching and learning perspective. 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 students 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. Additionally, any device with cellular connectivity is defined as a mobile phone even if the SIM card has been removed. If you are unsure whether your device is captured by this policy please check with the school's e-safety coordinator. These devices are referred to as 'mobile devices' in this policy.

This policy is supported by the 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.

For many young people today the ownership of a mobile phone/digital device is considered a necessary and vital part of their social life. When used creatively and responsibly the smart phone/digital device has great potential to support a pupil's learning experiences. What we are trying to achieve at Giggleswick is always a culture of respect for each other's privacy as well as promoting face-to-face interaction across the school.

Policy statements

1. Use of mobile devices at the school

Pupils are allowed to bring mobile devices into school. If they choose to do so it is on the understanding that they agree with the following limitations on its use, namely:

Students may use their own mobile device in the following locations:

- In the classroom with the permission of the teacher
- In the school environs - libraries, common rooms, boarding houses, etc.

Students may not bring any mobile devices in the following locations:

- Changing facilities

- School dining room
- Examination rooms
- Mobile phones should not be used by pupils or be visible anywhere around the school between the hours of 0820 and 1800 Monday-Friday and from 0820-1145 on Saturdays (except defined areas within Houses), or in public areas at all other times. There is no requirement for mobile phones to be used in lessons.
- The mobile device must be kept out of sight in public areas, e.g. the Flat, the dining hall and the library, unless it is being used as a learning resource.
- When use of a mobile device in lessons has been sanctioned, pupils must use it positively and for the agreed task. Disrupting the learning of others through use of the mobile device will not be tolerated.
- Mobile device use in houses will be at the discretion of the Housemaster or Housemistress.
- If asked to do so, content on the mobile device (e.g. messages, emails, pictures, videos, sound files) will be shown to the designated members of staff.
- Mobile devices should be handed in to the duty staff overnight in Y7-10, as per the school rules.

Students 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. Reception 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.

The school reserves the right to refuse students 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 students 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 students use it at their own risk. In particular, students are advised not to use the wireless network for 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. 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, students 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.

Students who receive any inappropriate content through school IT services or the school internet connection should report this to the school's IT team or a member of teaching staff as soon as possible.

4. Misuse of mobile devices

The following are examples of misuse but are not exhaustive. 'Misuse' will be at the discretion of the Headmaster:

- the deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass and intimidate by publishing to a wider audience via social media.
- bullying by text, image and email messaging
- the use of a mobile device for 'sexting' (the deliberate taking and sending of provocative images or text messages)
- pupils posting material on social network sites with no thought to the risks to their personal reputation and sometimes with the deliberate intention of causing harm to others
- making disrespectful comments, misrepresenting events or making defamatory remarks about teachers or other pupils
- general disruption to learning caused by pupils accessing mobile device in lessons
- the use of mobile devices in public areas which is affecting the social interactions of the students and staff at Giggleswick School
- pupils phoning parents immediately following an incident so that the ability of staff to deal with an incident is compromised
- publishing photographs of vulnerable pupils, who may be on a child protection plan, where this may put them at additional risk.

Dealing with breaches

Misuse of the mobile phone/digital device will be dealt with using the same principles set out in the school behaviour policy and the school rules, with the response being proportionate to the severity of the misuse.

Pupils are aware that misuse may lead to the confiscation of their mobile phone/digital device, communication with parents and the imposition of other sanctions up to and including exclusion from school. If the offence is serious it will be reported to the Police.

Where it is deemed necessary to examine the contents of a mobile phone/digital device this will be done by a designated member of staff (Headmaster/Deputy Head/Senior Master), and should follow the protocol of searching any pupil's possessions.

The action will be properly recorded in case it later becomes evidence of criminal activity. The record will include the time, who was present and what is found.

Unacceptable use

The school will consider any of the following to be unacceptable use of the mobile device and a serious breach of the school's behaviour policy, resulting in sanctions being taken.

- Photographing or filming other pupils or members of staff without their knowledge or permission
- Photographing or filming in toilets, changing rooms and similar areas
- Bullying, harassing or intimidating staff or pupils by the use of text, email or multimedia messaging, sending inappropriate messages or posts
- Refusing to switch a mobile device off or handing over the mobile device at the request of a member of staff
- Using the mobile device outside school hours to intimidate or upset pupils and staff will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time
- Using a mobile device outside school hours in such a way that it undermines the stability of the school and compromises its ability to fulfil the stated aim of providing 'a clear moral and ethical lead'.

Sanctions

Pupils and parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines, following the school's behaviour policy. In addition:

- pupils and their parents should be very clear that the school is within its rights to confiscate the mobile device where the guidelines have been breached.

Using the mobile phone/digital device outside school hours to intimidate or upset pupils and staff or undermine the stability of the school in any way will be considered a breach of these guidelines in the same way as unacceptable use which takes place in school time.

- If a phone/digital device is confiscated, school will make it clear for how long this will be and the procedure to be followed for its return.

- Pupils should be aware that the police will be informed if there is a serious misuse of the mobile phone/digital device where criminal activity is suspected
- If a pupil commits an act which causes serious harassment, alarm or distress to another pupil or member of staff the ultimate sanction may be permanent exclusion. School will consider the impact on the victim of the act in deciding the sanction.

Confiscation procedure

If a mobile device is confiscated, then:

- the pupil will be informed that the mobile device can be collected at the end of school day from the appropriate Housemaster/Housemistress or the Deputy Head/Senior Master.
    - *For the use of a phone between restricted hours:*
    - 1st offence – returned that evening at 1800
    - 2nd offence – returned the following evening at 1800 (parents/guardians informed)
    - 3rd offence – returned after three days at 1800 (parents/guardians informed)
    - 4th offence – parents/guardians invited into school and phone ban imposed.
- the confiscation will be recorded in iSAMS log for monitoring purposes
- school will ensure that confiscated equipment is stored in such a way that it is returned to the correct person
- in the case of repeated or serious misuse the mobile device will only be returned to a parent/guardian who will be required to visit the school by appointment to collect the mobile device. This may be at the end of a week, a half term or longer. At the discretion of the Headmaster the mobile device may be returned to the pupil at the end of the confiscation period.
- where a pupil persistently breaches the expectations, following a clear warning, the Headmaster may impose an outright ban from bringing a mobile device to school. This may be a fixed period or permanent ban.

Where the mobile device has been used for an unacceptable purpose

- The Headmaster or a designated staff member (Deputy Head/Senior Master) will have the right to view files stored in confiscated equipment and if necessary, seek the cooperation of parents in deleting any files which are in clear breach of these guidelines unless they are being preserved as evidence.
- If required evidence of the offence or suspected offence will be preserved, preferably by confiscation of the device and keeping it secure or by taking photographs of the screen.
- School will consider whether an incident should be reported to the safeguarding board.
- The designated staff member should monitor repeat offences to see if there is any pattern in the perpetrator or the victim which needs further investigation.

5. Security of student mobile devices

Students 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.

Students must never attempt to bypass any security controls in school systems or others' own devices.

Students are reminded to familiarise themselves with the school's e-safety, and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Students 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 Act 1998 and GDPR. Staff must apply this BYOD policy consistently with the school's Data Protection Policy.

7. Support

The school takes no responsibility for supporting student's own devices; nor has the school a responsibility for conducting annual PAT testing of personally-owned devices.

8. Incidents and Response

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

Reviewed by:	A Simpson, Deputy Head J Hamilton, Director of Digital Strategy J Mundell, Head of Junior School
Review period:	Annual
Updated:	February 2020
Approved by:	Governors' Pastoral & Boarding Committee, March 2020
Next review date:	February 2021