

I.T. ACCEPTABLE USE POLICY: Pupil use

Educational Mission Statement

Barfield School will provide an outstanding educational experience of the highest quality, within a safe and stimulating environment.

The purpose of this document is to make clear the expectations for safe and responsible use of ICT resources at Barfield School by pupils.

1. Guidelines for Pupils
 - 1.1. Security and Data Protection
 - 1.2. Conduct
 - 1.3. Privacy
 - 1.4. Appropriate use of Social Networking/Media Sites and Online Safety
 - 1.5. Reporting Problems
2. Mobile Devices
 - 2.1 School Devices and pupil owned device
 - 2.2 Off-Site Use of School Devices and Pupil Owned Devices
3. Consequences for Misuse/Disruption
4. School Liability Statement

1. Guidelines for Pupils

The School will provide Chrome devices and parents will be expected to provide Chromebooks (model to be specified each year) when their child enters Year 3, or joins the School after Year 3, for use by pupils as an important tool for learning. All pupils have a responsibility to use the School's I.T. network, or any other I.T. resources or devices at School in a respectful, lawful, and ethical manner. Pupils are expected to apply their knowledge of the taught principles of online safety at all times and are expected to abide by the School's conditions of use.

1.1 Security and Data protection

The School provides a filtered Internet connection for use by pupils as directed by staff. The filters are used both passively to block users from accessing inappropriate websites/fora and proactively to identify the use of a library of keywords by users of the school equipment which can then be acted on quickly and efficiently to prevent access to inappropriate websites including those that include terrorist and extremist material.

1.2 Conduct

School I.T. equipment, whether school owned or pupil owned, is provided for educational use only. Pupils must not use School I.T. equipment to play non-educational games.

Students shall make no attempts to circumvent the School's network security. This includes setting up proxies and downloading programs to bypass security.

Students shall only use devices while under direct supervision. The only exception to this is when a school or pupil owned Chromebook is being used at home to complete prep (**see section 2.2**). Whenever a pupil is logged into their device they are being monitored and the content they are able to access is filtered by GoGuardian.

Students are not permitted to use any device with a camera facility to take pictures or video in School or on a School trip or activity **AT ANY TIME**. (In special circumstances, pupils **may** be allowed to bring a digital camera on a school trip. E.g Brecon and the French Trip)

Pupils shall not distribute pictures or video or any other material relating to students or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting an image or video online).

The use of devices should not be a distraction in any way to teachers or students. Use of such equipment or devices must not disrupt class or private study areas in any way. Playing games or other non-School work related activities are not permitted.

If pupils use devices in a manner deemed unacceptable, then the School will consider suitable sanctions as per the *Behaviour Management Policy*.

1.3 Privacy

Pupils should not disclose any of their login details or passwords to anyone else.

Pupils should not attempt to gain access to another pupil's login data.

Pupils use of devices will be subject to monitoring by the School to ensure compliance with this Acceptable Use Policy and applicable laws.

1.4 Appropriate use of Social Networking/Media Sites and Online Safety

Pupils are strongly advised to not use any social networking site or pages in any way that may compromise their current or future education at the School. Any content that pupils post about themselves or others could be brought to the attention of the School and may be detrimental to future studies and/or career.

Pupils should take effective precautions when using social networking sites to ensure their own personal safety and to protect against identity theft.

Pupils must not use any social network site to attack, abuse or bully any School staff, other pupils or people. The privacy and the feelings of others should be respected at all times. Pupils will be required to remove internet postings which are deemed to constitute a breach of this policy.

Pupils must not include contact details or pictures, etc. of other pupils or members of staff without their prior permission. You should never reveal confidential information about the School, staff or pupils. Please consult with your Form Tutor if you are unclear about what might be confidential.

Pupils need to consider intellectual property rights, copyright and ownership of data when using social media. You should exercise caution when interacting with, and responding to, potentially contentious posts on social media sites.

Pupils are strongly advised to Follow Childnet's **SMART** Rules when using Social Media sites:

Safe. Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address, or School name - to people whom you don't know or trust online.

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

Accepting emails, instant messages, opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages.

Reliable. Someone online may be lying about who they are, and information you find on the Internet may not be reliable.

Tell your parents, carer or a trusted adult if someone or something makes you feel uncomfortable or worried.

1.5 Reporting problems

Any problems arising should be referred to the member of staff leading the class who should inform the Director of Technology at the earliest opportunity.

Pupils who have lost documents or files should report this as soon as possible.

2. Mobile Devices

2.1 School Devices and pupil owned devices

Both School Chrome devices and pupil owned Chromebooks are provided for students educational use in lessons and during Prep.

Chromebooks should be treated with care whilst being carried around School and, when not in use, should be stored in a safe location.

When a pupil has finished with a Chromebook, it should be returned to its case and stored in a safe location.

2.2 Off-Site Use of School Devices and Pupil Owned Devices

Pupils will be expected to charge their Chromebook at home, bringing their Chromebook to school fully charged each morning. Chargers should not be brought to school.

Pupils are allowed to connect their Chromebook to their home wifi network to allow them to complete school work such as prep at home. However, all the guidelines listed in this document apply at home. Particularly (but not limited to) section **1.2 Conduct**.

It is expected that the Chromebook provided to each pupil is treated with the utmost care, both at School and at home - any damage should be immediately reported to the Director of Technology.

Barfield School reserves the right to bill pupils who cause damage to their School owned Chromebook through misuse.

2.3 Personal Devices - other than Chromebooks (Only by prior agreement with the Director of Technology in consultation with the SMT)

Pupils are **not permitted to connect their Personal Device to any mobile networking service.** Any capabilities that the device has to achieve this should be turned off while in school. Personal Mobile Devices may be connected to the School's wireless network in some circumstances, with permission from the Director of Technology.

In the case that agreement has been reached that a pupil may bring in a Personal Device, there are no secure facilities provided at School to store Personal Mobile Devices. Students take sole responsibility for the safekeeping of their devices while in school.

Use of Personal Devices during the school day is at the discretion of teachers and staff. Students must use devices as directed by their teacher.

Students must check their Personal Device daily to ensure the device is free from unsuitable material and free from viruses etc. before bringing the device into school.

Any power leads that are brought into School must have been PAT tested by a company approved by the School. If in any doubt please contact the Director of Technology.

Students must check their Personal Device daily for basic Health and Safety compliance to ensure it is free from defects. Particular attention should be paid to the power lead (lead not frayed; plug correctly fitted and containing the correct fuse rating), the keyboard (all keys present; no bare metal exposed), the screen (free from flicker and damage) and the device battery (able to hold a charge). Any Personal Device that has obvious Health and Safety defects should not be brought into School. Pupils are expected to take responsibility for the printing of any work, under the guidance of the Head of ICT/ICT teachers.

3. Consequences for Misuse/Disruption

In addition to dealing with misuse/disruption within the remit of Barfield School's I.T. Acceptable Use Policy and the School's Behaviour Management Policy one or more of the following sanctions may apply (but are not limited to):

- The device would be confiscated and kept in the Front Office until the parent/guardian picks it up.
- Privilege of using School I.T. equipment or Personal Devices at School would be removed.
- Misuse of Internet capable devices is regarded as a serious offence as it is in direct contravention of Barfield School's I.T. Acceptable Use Policy and Behaviour Management Policy and will be dealt with in accordance with these policies.

4. School Liability Statement

Students bring their personal devices to use at Barfield School **at their own risk**. Students are expected to act responsibly with regards to their own device, **keeping it up to date via regular antivirus and operating system updates and as secure as possible**. It is their duty to be responsible for the upkeep and protection of their devices.

Barfield School is in no way responsible for:

- Personal devices that are broken while at school or during School-sponsored activities.
- Personal devices that are lost or stolen at school or during School-sponsored activities.
- Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).
- Parents should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of a personal ICT device in the event of loss/damage to the device.
- Content accessed by pupils through non-School controlled wireless Internet systems such as (but not limited to) 3G/4G/5G/'Wireless Hotspots'.

Disclaimer

Barfield School accepts no liability in respect of any loss/damage to personal devices while at school or during school-sponsored activities. The decision to bring a personal device into school rests with the student and their parent(s)/guardian(s), as does the liability for any loss/damage that may result from the use of a personal device in school. It is a condition of agreeing to allow students to bring personal devices into School, that the parent/guardian countersigning the permission slip accepts this disclaimer.

Declaration

Please refer to the letter sent to you by Mr Taylor via email on the 16th September 2022.

Within his letter, you will find a link to click, to be taken to the **Online Declaration Form**.

As this declaration forms part of our compliance procedures, kindly complete the form and submit your response by no later than the 23rd September 2022.