

"Bring Your Own Device" (BYOD) Policy

The "Bring Your Own Device (BYOD)" approach provides an additional resource within the curriculum. School recognises the benefits to learning from offering students the opportunity to use tablets, laptops and other ICT devices in school to support learners and their learning. By using any such device in school, students agree to be bound by the additional school rules and requirements set out in this policy.

It is not the School's responsibility to provide or support personal student devices. The use of personal ICT devices falls under the online safety policy (and acceptable use policy) which all students must agree to, and comply with. Students are not permitted to connect to any external wireless or networking service (e.g. 5G/4G/3G/GPRS, etc.) while using a personal ICT device in school.

The use of a personal ICT device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt class or Private Study areas. Playing games, accessing social networks or other non-school academic related activities are not permitted during lessons or in any area other than the Common Rooms, for Sixth Form.

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

The School is in no way responsible for:

- Personal devices that are broken whilst at school or during school-sponsored activities.
- Any data lost on personal devices.
- 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.

Please note that the School has in the past taken serious disciplinary action (e.g. exclusion) in response to offences which originated outside of the School's IT facilities but which impinged on the School or affected members of the School community. This would include, for example, the use of social media in a manner which could harm the reputation of the School or could cause harm to others.

BYOD and Mobile Phone Policy

The use of mobiles in school follows the school behaviour policy. Most students have access to 4G and 5G networks with the associated dangers of restricted sites and cyber-bullying. Mobile phones should not be used in School, except under the express permission of a member of staff. Year 7 to 10 will hand their mobile phones to their Form Tutor in morning registration and receive them back at the end of the day. If students do not have a mobile telephone, or do not bring it in to School, this needs to be confirmed in writing by a parent to the Form Tutor. Students in Year 11 should have their phones switched off and out of sight throughout the school day. In 6th Form, students may have their phones and may use them in the 6th Form Common Spaces at the discretion of the Head of 6th Form.

Contravention of these rules will result in the device being confiscated for at least 24 hours, and over the weekend in the case of the device being confiscated on a Friday. Depending on an individual student's weekend circumstances, Heads of Year may arrange alternative consequences at their discretion. Mobile 'phones will not be returned to a student, they must be collected by a parent.

Searching and Screening Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.



When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- **>** Break any of the school rules

>

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*
- * Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on <u>sharing nudes and semi-nudes</u>: <u>advice for education settings working with</u> children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headmasters and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the <u>Education Act 1996</u> (as amended), the <u>Education and Inspections Act 2006</u> and the <u>Equality Act 2010</u>. In addition, it reflects the <u>Education Act 2011</u>, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.



Online Safety in School

When using devices in school, these must be connected to the School's wi-fi. The wi-fi is monitored for any harmful searches by a filtering system called Smoothwall. Harmful sites are blocked, and searches made by students which may indicate a safety concern are flagged to the network manager, and the Designated Safeguarding Lead and dealt with appropriately.

Safe Usage Advice for Students:

- Be careful to whom you give your mobile phone number and never post it on websites.
- Never return a call or text message to a number you do not know.
- Never reply to texts saying you have won prizes. These are usually based around premium rate numbers and may cost you a small fortune.
- If you are using text chat, make sure your username does not give away your real name.
- If you receive abusive text messages, keep them. You do not have to read them. When the time comes to take action, these messages can be used as evidence.
- If you receive abusive text or chat messages, ask for help from your Form Tutor, Head of Year, the School Nurse, a parent or any trusted adult. You can also contact your mobile phone provider.
- Remember, by forwarding a text, email, photo, video, etc. you may be making a problem worse. You could be unwittingly involving yourself in bullying. You may even be breaking the law. It is illegal to share explicit images, or send any explicit images (including those of yourself).

Reviewed by Graham Murdoch 2nd June 2025

To be reviewed June 2026