

Marling Sixth Form BYOD Policy

At Marling Sixth Form, we embrace the transformative power of technology in education and are proud to make use of technology in all aspects of learning. Our sixth form digital policy is designed to harness the benefits of digital learning, providing students with the flexibility to engage with educational resources and collaborate in ways that transcend traditional classroom boundaries. Our policy supports personalised learning experiences, allowing students to utilise devices they are familiar with, thereby enhancing their learning efficiency and digital literacy whilst allowing us to support out students. A fundamental part of this policy will allow Marling Sixth form to effectively safeguard our students and support their welfare with regards to monitoring and filtering as underpinned by statutory safeguarding protocols. Sixth Form students can make a request to join the school network with a personal device (not mobile phone) in line with the requirements detailed in this policy and only those accepted requests will be granted access. Students and parents/carers must sign the BYOD User Agreement which Marling Sixth Form reserves the right to withdraw or deny access if students do not follow the broader Student IT Acceptable Usage Policy (AUP).

Related digital policies:

- **ICT and Internet Acceptable Usage Policy (AUP)**
- **Mobile Phone Policy**

BYOD Student Guidelines

Before being granted the additional privilege of accessing the school's network via a personal device, students must have read and thereby agreed to comply with Marling School AUP when using the school computers. The use of a personal device at school must be for educational purposes only.

Students must not allow others to use their device for any purpose whilst connected to the network (including, but not limited to, the Internet). If a student suspects another person may know their password, they must get it change it immediately either by requesting a password change on mylogin or by speaking to their tutor.

Students are responsible for the safety of their device and no secure facility will be provided to store their personal device at school. Students should always keep their personal device with them. The use of a personal device during lessons is at the discretion of teachers or staff; students must use their device as directed by the teacher or member of staff. Personal devices must not disrupt the class, others, or Private Study areas in any way. Non-schoolwork-related activities are not permitted.

Students must make no attempt to circumvent the school's network security or internet filtering; this includes, but is not limited to setting up proxies, MAC address spoofing, use of a VPN or using programs to try to bypass security. Students are prohibited from accessing any other network whilst at school.

Students must not upload/distribute pictures or video or any other material relating to students or staff without their permission. This includes, but is not limited to, emailing/snapchatting/messaging an image or video to posting an image or video on a social networking site.

Students are responsible for ensuring their personal device is free from viruses (and virus definitions kept up to date) and unsuitable material before bringing the device into school.

Students are responsible for checking their device daily for any Health and Safety issues, to ensure it is free from defects. Items such as the power lead/charging pack must not have crimped/split wiring, must have the correct fuse fitted and should be in good working order. The battery must be in good health and hold charge as we do not have dedicated facilities for charging in school. Any defects must be rectified before being used in school.

Sanctions

In addition to the sanctions stated in the school's Acceptable Use Policy and the school's Behaviour Policy, one or more of the following sanctions may apply:

- The device will be confiscated until a parent/guardian comes into school to collect it.
- The privilege of using a personal device in school will be removed.
- Banned from using the school's network and other connected hardware.

School Liability Statement

Marling School can in no way be held responsible for loss or damage to a personal device brought into school; students do so entirely at their own risk. Responsible use, by the student, is paramount and is expected at all times, including but not limited to: keeping it up to date via regular anti-virus and operating system updates and as secure as possible. It is the student's duty to be responsible for the upkeep and protection of their devices.

Marling School is in no way responsible for:

- Any personal device that is broken whilst at school or during school-led activities.
- Any personal device that is lost or stolen at school or during school-led activities.
- The maintenance or upkeep of any device (charging, updating or upgrading, fixing software or hardware issues).
- Any other technical support with regard to a BYOD and the network connection
- The insurance of any device brought into school. This is the sole responsibility of parents/guardians and must provide adequate cover for the cost of repair/replacement or, in the respect of loss/theft of the device

School Disclaimer

Marling School will not accept any liability for any loss/theft/damage to any personal device on route to, during, on the route home from school or school-led activity. Final permission to allow a personal device into school rests with the Head of Sixth Form, but the final decision to bring a personal device into school rests with the student and their parent(s)/carer(s), as does the liability for any loss/theft/damage whilst the device is used in school or on a school-led activity. Marling School and our IT providers accept no liability for any hardware or software issues linked to connecting to the wireless network. A parent/carer must countersign the online form, at the end of this policy/agreement before it will be accepted and a device allowed to be brought into school. Marling School and Lift Schools, IT are unable to give technical assistance with personal devices beyond connecting to the WiFi network.

Frequently Asked Questions (FAQs)

What type of personal device can a Sixth Former bring into school to connect to the school network?

A laptop or a tablet only. Smart phones/mobile phones/phablets (phone/tablet hybrids) are NOT permitted nor will any other type of device be permitted. No other device is permitted.

What is a MAC address and why do I need to share it?

A MAC address is a unique address which identifies your device. This is programmed by the manufacturer and can be found in the settings of your device. Marling School will use your MAC address to identify your network traffic to allow us to effectively monitor use internet usage when connected to the school network. You can use the following link to support you finding your device's MAC address: <https://tinyurl.com/5n6decnb>

How will I connect to the School WiFi?

Students using BYOD are permitted to connect to the BYOD Wi-Fi network. Once the agreement has been signed, students will receive an email with instructions on how to login, as part of this, students will need to download a certificate to their device which will allow Marling School to filter the internet. Students will need to login with their school email and password to use the wifi network. Only those students who have signed all parts of the policy will be granted access to the network. Internet logs will be monitored by Marling School for safeguarding reasons.

Can I transfer work from school computers to my personal ICT device?

Students should use their Google Drive to transfer files between personal devices and the school network. USB sticks have been prohibited from use on the school network as part of Cyber Security policy.

Can I access another wireless network or networking service while in school?

Students are not permitted to use other wireless technologies to connect to the Internet; this includes, but is not limited to: 3G networks, wireless hotspots etc. Any student accessing such a network would be committing a breach of trust and would no longer be able to use a personal device in school.

Can I use my personal ICT device in class?

Devices may only be used in class with the approval of the class teacher.

Will IT be able to support me with technical issues on my device?

IT will be unable to support students beyond connecting their device to the school network. Students and parents that are looking for a fully supported device should look at our device lease scheme.

How do I transport my ICT device?

It is recommended you use a well-padded laptop bag for laptops, or a padded sleeve or protective case for tablet computers.

What software should I use for my work?

You will be able to use your school login to access your work on Google Drive, Docs and Slides.

What if I get a new device?

If you would like to connect a new device to the school network, it is your responsibility to re-sign the BYOD agreement which will allow us to update our systems to allow your new device on the network and remove the old one.

What are my responsibilities as a student?

You are fully responsible for the safety, security and proper use of your own personal device at all times. There are no secure facilities provided at school to store your personal device. You should therefore keep your personal device with you at all times.

- You must use the device for educational/learning purposes only.
- You must charge the device prior to bringing it into school.
- You must ensure antivirus and operating systems are updated regularly on the device.
- You must care for the device and ensure it is kept safe and secure.
- You must check the device for viruses and unsuitable material daily prior to bringing the device into school.
- You must abide by the Bring Your Own Device (BYOD) Policy, the Acceptable Use Policy and the Behaviour Policy.

How will my BYOD device be monitored?

All internet traffic will be monitored in relation to keywords as part of our Safeguarding policies with alerts sent to the DSL and wider Safeguarding team. All internet activity is monitored by Marling School whenever a student is signed in to their school Google account, regardless of whether they are connected to the BYOD network.

If you have any questions about this policy please contact either:

Ms Louise Harris – Head of Sixth Form

Mrs Catherine Lee – Digital Learning Lead

Marling School Student Acceptable Usage Policy - September 2026



This student friendly policy is adapted from the ICT and Internet Acceptable Use Policy and Artificial Intelligence policy.

Purpose

This Acceptable Use Policy (AUP) outlines the guidelines and expectations for the appropriate use of technology and digital resources at Marling School. Our goal is to ensure a safe, respectful, and productive learning environment for all students.

Respectful Use

Students must use technology in a manner that is respectful to others and the school community. Cyberbullying, harassment, or any form of disrespectful communication is strictly prohibited and will be dealt with in line with the school's behaviour policy. Students are expected to practice good digital citizenship by being mindful of their online behaviour and the impact it can have on themselves and others. Plagiarism and academic dishonesty are not tolerated. Students must properly cite sources and create original work.

Educational Purpose

Technology resources are to be used primarily for educational purposes, including research, assignments, and projects. Downloading or sharing copyrighted material without permission is prohibited.

Access to IT Resources and Facilities

Computers and equipment in Marling School's IT suites are available to pupils only under the supervision of staff. Specialist IT equipment, such as that used for Music, Art and Design Technology must only be used under the supervision of staff. Sixth Formers may use computers and equipment independently in the study rooms for educational purposes only and in line with this Policy.

Students are responsible for the care and maintenance of any school IT equipment including devices. Any damage or technical issues should be reported to the IT team immediately. If students are found to be responsible for damage or loss of equipment, there may be a charge to parents/guardians in line with the school's behaviour policy.

Monitoring

The school monitors all activity by students on both school IT equipment and student devices which includes their use outside of school. This includes activity and access logs, internet sites visited and electronic communication. Concerns raised by staff or IT will be passed on to the Safeguarding team and sanctioned in line with the behaviour policy.

Privacy and Security

Students must respect the privacy of others and not access, modify, or share another person's files or data without permission. Passwords and login credentials must be kept confidential and not shared with others. Secure passwords should include upper and lower characters, numbers and symbols.

Student Devices

Our student device scheme allows students to purchase/lease a device through the school to use both at school and at home. These devices are monitored at all times. Sixth Form students have the opportunity to use personal devices (laptops/tablets) through our BYOD policy.

Internet Access

The school's internet is secure and filtered. Students should not make any attempts to circumvent the filters including but not limited to the use of a 4G hotspot or VPN.

Artificial Intelligence

AI-powered tools can provide personalised learning paths, helping students grasp complex subjects at their own pace. Using AI to commit plagiarism undermines the integrity of the educational process and violates academic honesty policies. Students should avoid using AI tools to generate or copy content without proper attribution, as this can lead to sanctions in line with the school's behaviour policy. There are serious consequences for using AI without referencing as part of NEA (Non-Examined Assessment) at KS4 and 5.

Unacceptable use

Examples of unacceptable use include but are not limited to:

- Using the ICT facilities to breach intellectual property rights or copyright
- Using the ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust or School's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Downloading or setting up any software, applications or web services on the Trust's network without approval by the IT
- Services Team, or creating or using any programme, tool or item of software designed to interfere with the functioning of the Trust's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel

- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities
- Removing, deleting or disposing of the Trust's ICT equipment, systems, programmes or information without permission from authorised personnel
- Using inappropriate or offensive language
- Using websites or mechanisms to bypass the Trust's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

Sanctions

Students who engage in any of the unacceptable activity listed may face a sanction in line with the school's behaviour policy.

Marling Sixth Form – Bring your Own Device (BYOD) User Agreement

Please complete the Microsoft Form with your son/daughter. Please make sure that you have both read and understood the Acceptable Usage Policy and the BYOD Policy (above) before completing the form. Following completion of the user agreement, the details will be passed to our IT team who will grant access to the network in line with the detail in this policy.

[Sign BYOD User Agreement](#)