



Bring Your Own Device Policy (BYOD) 2025-2026

This policy sets out how Northleigh (the School) manages students who bring their own device(s) to school and make use of this device(s) for school and educational purposes. Throughout this policy the word 'device' is used to describe any mobile phone, tablet, portable computer, or any other devices capable of connecting to the internet.

The use of devices at school deepens learning, is personalised and student-centred, helps to develop modern teaching and learning practices, and fosters digital literacy, fluency and social responsibility in a safe environment.

This policy is one of several safeguarding policies, all of which are in place to protect and promote the welfare of our students. This policy should be read in conjunction with the following documents:

- Student Acceptable Use Policy
- Child Protection and Safeguarding Policy
- Filtering and Monitoring Policy
- Online Safety Policy
- DfE: Keeping Children Safe in Education Mobile Phones and Smart Watches

Students are only allowed to use their mobile phones or Smart watches before or after school, but not on the school premises during school hours. Exceptions may be possible on a case-by-case basis e.g. for medical, SEND purposes, etc.

The "Bring Your Own Device (BYOD)" approach provides an additional resource within the curriculum. The School recognises the benefits to learning by 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.

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 on the school site unless within a learning environment.

Students bring their personal ICT devices to use at the 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 may take serious disciplinary action (e.g. exclusion) in response to offences which originated outside of the School's IT facilities but which impinge on the School or affect 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.

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 the School, except under the express permission of a member of staff. Students are to hand their mobile phones into a member of staff upon entry to the school at the beginning of the school day. Mobile phones will be returned at the end of the school day.

Mobile phones may be taken on school trips, but these must be used responsibly. If student(s) are found to have a mobile phone which has not been handed in at the beginning of the school day, the device may be confiscated and returned at the end of the school day.

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 sharing nudes and semi-nudes: advice for education settings working with 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.

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 system called Securus.

Harmful sites are blocked, and searches made by students which may indicate a safety concern are flagged to the Wellbeing Mentors, and/or the Designated Safeguarding Lead and dealt with appropriately.

We advertise the GUEST wi-fi to stop students trying to get access to main School wi-fi. The Guest wi-fi has filters on it which are the same as student logins.

ONLY devices registered to the Northleigh domain will be monitored (this also excludes school MACs) & filtered.

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.

Updated 28.01.2026

- 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 wellbeing mentor, the school director, 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).

Review Date – September 2026