

IT Acceptable Use and Online Safety Policy

Senior School Pupils

The policy provides guidance regarding what is and what is not acceptable use of the electronic media and systems provided by the School.

The following regulations apply to all electronic media, including but not limited to mobile / smart technology and services that are:

- Accessed on or from the School premises
- Accessed on School equipment
- Accessed via The School Network
- Accessed via The School’s online portals (e.g. M365 or HERO)
- Or are used in a manner which identifies the individual user with the School

1. School Equipment	1
2. Personal Devices	2
3. Office 365	3
4. Wi-Fi and Networking	3
5. Online Conduct	4
6. E-Learning	4

1. School Equipment

- Except for portable devices, IT equipment must not be moved, relocated or adjusted without the permission of a member of staff.
- Screens and projectors in classrooms and other areas of the School must not be touched without the permission of a member of staff.
- No software or programs may be installed by pupils on any School computer/device.
- Printers at school must only be used by pupils for legitimate academic or co-curricular activities at Highgate School. Pupils should consider the necessity of printing material in accordance with responsible environmental awareness.
- Damage to IT equipment, whether accidental or otherwise, must be reported to a member of staff immediately.

- When using a School owned portable device (e.g. an iPad), pupils may not record or take photos except with the explicit permission of a member of Staff. They should not change any settings on the device. If pupils do so, they may be subject to disciplinary sanctions.
- The use of portable storage devices (e.g. USB memory sticks and hard drives) to connect to School IT equipment is prohibited. Failure to comply may be subject to appropriate disciplinary sanctions in accordance with the School's Behaviour Policy.
- Any deliberate attempt to damage or 'hack' into the School's IT infrastructure or online services will result in disciplinary action in accordance with the School's Behaviour Policy (this may include temporary or permanent exclusion from School).

2. Personal Devices

- The acceptable use of mobile phones and other personal devices in the Senior School is detailed in the School Rules (as detailed in Section 6.2 of the Behaviour Policy).
- Mobile phones (and other personal electronic devices such as tablets) must not be brought out or used (visibility is taken as usage) between the point of arrival at school and the end of the school day (usually 4pm) whilst on the school site, or while travelling between parts of the site (including the road crossings and St Michael's Path and the), in line with the school's Behaviour Policy. Exceptions for Sixth Form Pupils in some circumstances are detailed below.
- After the end of the school day and until 4.20pm, pupils may use their Mobile Devices for communication with parents and essential travel plans, but no other purpose. The end of the school day should be taken to mean the end of routine school activities on a given day, so Mobile Devices should not be used by pupils attending after-school Clubs, Training or School Omegas and Detentions.
- Smart Watches and similar Wearable Devices may be worn, though their Smart functions should not be accessed during the times detailed above (it is recommended that pupils use Aeroplane Mode or Do Not Disturb Mode).
- For pupils in Sixth Form, Mobile Devices and Headphones may be used discreetly in the Library, Study Rooms and Sixth Form Common Rooms. Pupils' use of electronic devices in the Library and Study Rooms should be restricted to legitimate academic work.
- Additionally, with prior permission from a teacher, pupils in Sixth Form are permitted to use Laptops, Tablets and Mobile Devices in lessons, in line with the school's Sixth Form BYOD policy. Use of Laptops and Tablets for legitimate academic work is also permitted in the locations detailed above.
- A Teacher or member of the Support Staff (e.g. the School Nurse or a member of the Learning Support Department) may give a pupil specific permission to use their mobile device, either for essential health monitoring (e.g. blood-sugar level tracking) or other exceptional pastoral purposes.
- It is not permitted to take (or distribute) films or images of anyone during the school day using any device, except in exceptional circumstances as part of a school activity led by a member of school staff; any pupil doing so without staff permission will be subject to disciplinary action. Should pupils upload such images to social media this will be considered a serious disciplinary breach.
- Any use of personal mobile technology which is not in line with the above will result in devices being confiscated and sanctions applied, in accordance with the School's Behaviour Policy. The School rules are published termly and regularly reviewed and updated by Senior Staff and the Pupils' School Council.

- All pupils should be aware of the personal safety risk of using mobile devices in an urban environment on the journey to, from and around the School Site. Pupils should protect themselves and their property by appropriately selective and discreet use of Mobile Devices and Wearable Technology as they arrive and depart from School.
- If pupils are in any doubt as to what this means for their use of an electronic device in any given circumstances then they are encouraged to speak to a member of staff.

3. Office 365

- Every pupil has an online account issued to them by the School. Pupils must use their email account when emailing members of staff at Highgate School. The School reserves the right to monitor pupil emails. Pupils should not add a personal photo to their profile. Pupils are prohibited from using associated messaging apps like Teams to contact staff or other pupils.
- Every pupil has a home OneDrive area to store private files and folders for schoolwork only. This home space (OneDrive) may not be used to store personal photographs, music or documents. This home space is backed up regularly to protect against data loss.
- Pupil accounts and home spaces are password protected. Pupils should safeguard the security of their personal information by choosing appropriately robust passwords and not sharing their password with anyone. School passwords should be unique and not widely-used personal passwords. The use of passphrases is highly recommended, i.e. creating passwords using three random words. If the account appears to be compromised, pupils must notify the IT Department immediately by submitting the form, which is available on HERO (<https://hero.highgateschool.org.uk/hero/account-tampering>).
- Use of a School email address and access to the School's online services will be discontinued when a pupil leaves Highgate and is removed from the School roll. Unless otherwise indicated, School email addresses will be retained for use by leavers in Years 11 and 13 until August 31st in order to facilitate effective communication regarding examination results and the university application process. It is the pupil's responsibility to ensure alternative email arrangements are made prior to leaving Highgate, and to backup any personal files that they would like to retain on their home device.

4. Wi-Fi and Networking

- Wi-fi and the School network / IT facilities are provided for educational, research and personal development use of all members of the School community. Sixth Form pupils using their own devices in school should use the School's Wi-fi service for mobile internet access in accordance with the Sixth Form BYOD Policy.
- If pupils are found to be seeking out or accessing inappropriate sites that do not meet the educational objectives of the School by using personal LTS (e.g. 4G and 5G) services, they will be subject to appropriate disciplinary sanctions, in accordance with the School's Behaviour Policy.
- In line with the School's Prevent responsibilities and safeguarding purposes, the use of the School network is monitored and recorded (using the Securly platform) in order to ensure that pupils are not being subjected to online bullying nor are accessing material which encourages political extremism. All pupils are encouraged to think critically about any information that they find online and understand that not all information online is reliable. Pupils should discuss any concerns they may have with online material with a member of staff.

- Highgate School uses web filtering software to secure, monitor and limit certain websites for the security of all members of the school. However, if we have blocked a legitimate website, pupils should fill in the HERO form (<http://hero.highgateschool.org.uk/hero/website-reporting>) to inform IT Services.

5. Online Conduct

- As with all forms of bullying, the School regards cyber-bullying, through the inappropriate use of electronic communication such as text messages, email or postings on social networking websites, e.g. Facebook, Twitter, Snapchat, as unacceptable. This includes the use of technology outside of normal School hours if it interferes with the safety and well-being of any member of the School community, including staff. Such incidents will be treated seriously, investigated thoroughly and appropriate disciplinary measures taken if necessary. Full details can be found in the School's Anti-bullying Policy. Pupils can find more information and support guidance here <https://www.ceop.police.uk/safety-centre/>.
- In addition, pupils should not post on social media any content or comments which risk damaging the reputation of the School. Pupils who have concerns about an aspect of school life may report them via the Highgate Student Voice platform where they can be followed up directly by School staff.
- Youth Produced Sexual Imagery (sometimes referred to as 'Sexting' or nudes/semi-nudes) is an offence in law and is therefore regarded by the School as a serious concern. If the School is made aware that such images have been shared between or among pupils, then the School will follow the guidance issued by the UKCIS (as detailed in the School's Safeguarding and Welfare policy). In addition to following safeguarding procedures, the School is likely to regard such incidents as disciplinary matters.
- When posting on HERO, pupils should be aware about the impact their words may have on other users. Irony may not be obvious when read out of context, so comments should always be written with this in mind. If abuses are discovered, appropriate sanctions will ensue.

6. E-Learning

- HERO and the School's Intranet are provided for members of the Highgate School community only. Academic pages provide information and resources to support learning. Pupils are encouraged to engage with these facilities in a constructive and responsible manner. Any interactive activities, message boards or comment boxes must be used for designated educational purposes. Inappropriate comments or posting material that is illegal, likely to cause offence or breaches the School's Code of Conduct will result in disciplinary action, according to the School's Behaviour Policy. If pupils wish to delete any comments, or if they believe another member of the School community has accessed their accounts, they should report the incident to a member of staff, who will contact the Head of e-Learning or the IT services department.
- When using their School email to communicate with other pupils and/or members of staff, pupils must do this between the hours of 7am – 7pm, unless in an emergency. Pupils must also expect teachers to only communicate, via email or setting HERO tasks, between these hours.
- Pupils will be provided and are expected to complete online safeguarding training as part of their PSHEE lessons and attend talks (Childnet Y7 and Y9). This will cover: keeping safe online, password protections, sharing data, safe internet browsing and appropriate use of school resources. If pupils require extra support, please speak to a member of staff or follow links to online support via HERO. (<https://hero.highgateschool.org.uk/get-help-here>)

- When using School iPads and other School Device, pupils are instructed to sign into their Office 365 (OneDrive, Word etc.) account through any application. They must sign out of the applications at the end of the lesson or activity to avoid data loss and account tampering.
- Any deliberate attempt to tamper with the account settings on School owned devices e.g. changing a device name or signing into iCloud and enrolling certificates will be subject to appropriate disciplinary sanctions in accordance with the School's Behaviour Policy.