D'OVERBROECK'S
OXFORD
A NORD ANGLIA EDUCATION SCHOOL

ACCEPTABLE USE OF IT EQUIPMENT POLICY – STUDENTS

Last reviewed:	September 2025
Next review due:	September 2026
Reviewed by:	Head of IT (UK) Director of Digital Strategy

1. Purpose and scope

1.1 Introduction

This Acceptable Use policy sets out the approach of d'Overbroeck's relating to the minimum requirements that users are bound to when using hardware, software, internet and network equipment (together "IT systems") that is owned and operated by the school. This policy represents the minimum requirements that must be met by all students.

1.2 Scope

This policy has been prepared in accordance with the school's legislative requirements and principles. This policy is effective across the entire school and applies only to students ("users") of IT systems, including those users using privately owned computers that connect to the school network resources and applications.

2. Policy statement

2.1 Underlying principles

All users must adhere to all elements of this policy. The principles of behaviour relating to the use of the school's IT systems include:

- respect for appropriate legislation and regulations;
- respect for students and teaching staff; and
- respect for the school's aims and values.

The principles of conduct of users also expect:

- integrity
- diligence
- economy
- efficiency
- common sense

2.2 Role and responsibilities

All users of the school's IT systems have a responsibility to maintain compliance with this policy and all relevant policies. Additionally, all users have a responsibility to maintain security and to report anything that may be detrimental to the school. The Service Desk may be used (as per the arrangements for the school) for recording all incidents and allocating investigation or remediation work to core services as required

2.3 User accounts and passwords

- You are responsible for any activity that is performed while your network account is logged on. Do not share your password with any other person (including IT) and do not log in using any other user's credentials. Passwords are the "key" into the school's IT systems - it is your own responsibility to ensure your password is kept secure. Two key password management practices make it harder for attackers to access the school's systems and data.
- Use "Strong Passwords." These can slow down or often defeat the various attack methods used to compromise IT security. The school requires you to always use Strong Passwords. A Strong Password is not easily guessed (not your name, family members, pets, relatives or anything else that could be attributed to you). Passwords must be a minimum of eight characters long and contain a combination of upper and lowercase letters, numbers and special characters. Longer passwords (13+ characters) with less complexity (variation in character types) also increase the strength of the password. The stronger the password, the harder it is to guess or crack.
- Always use different passwords for different sites; whilst it's convenient to re-use the same password for personal logins, ensure your password is not one that you use elsewhere. Using a unique password for your user accounts ensures that systems remain secure if any of your personal accounts are compromised and vice versa.

2.4 Personal use of company computers and IT facilities

IT systems should not be used for anything other than academic pursuits.

- A network account is provided to a student for the period of their enrolment.
- Users are required to manage their allocated network and email storage quotas.
- Users are not to store personal data on school IT systems.
- Users must not lock IT systems, thereby preventing other users from accessing them.
- Users must not consume food or drinks around or near IT systems.
- Occasional use of the school's IT systems to access the internet is acceptable, eg, for checking the news, etc. The same applies to other IT facilities such as internet connectivity, printing, or scanning.
- School IT systems must not be used for the following:
    - gambling or Internet gaming;
    - any political activity;
    - sending offensive, harassing, intimidating or discriminatory messages or attachments, or transmitting offensive, sexually explicit or other inappropriate material;

    - downloading malicious software or applications;
    - browsing, sharing, downloading from, or otherwise accessing illegal websites or the use of online security scanning or hacking/cracking tools;
    - accessing IT systems for personal financial gain, solicitation, or personal business purposes, eg, crypto currency mining;
    - posting information on bulletin boards, blogs or forums that are accessible by the public unless you are specifically authorised to do so;
    - downloading or storage of data which would breach copyright laws;
    - representing school on social websites. Take care when posting pictures that they do not contain school information in the background and that you have permission from your school colleagues before posting any pictures of them.
- A specific agreement is required between the school and the consumer when it provides a service such as the internet for personal use.

2.5 No outside internet use

The school's IT systems are only to be used for academic purposes. The only exception is the occasional use permitted in 2.4 above. Any form of outside interest use is prohibited, unless the school has given prior written authorisation. This means that users of the school's IT systems must not use and must not allow any non-d'Overbroeck's person or organisation to access or use the school's IT systems, services and equipment for any purpose.

This includes but is not limited to the following types of actions:

- sending unsolicited emails to persons;
- using email or social media platforms to solicit interest in goods or services, participation in surveys, events or group activities or links to any third-party URL or hosted sites;
- data mining for personal information, including email addresses, telephone numbers, social media profiles or other personal information that may be stored or accessible on the school's system.

2.6 Equipment, security and loss

IT equipment and devices must be treated with respect. Do not leave any equipment unattended where it could be stolen or abused. Users are personally responsible for all equipment issued to them by the school. Lost or stolen equipment must be immediately reported to the school through the it.servicedesk@nordanglia.com

Hardware always remains the property of the school and when a student comes off the school roll any loaned equipment must be returned to the school in a clean, tidy, working and prompt fashion. All devices, ie, tablets, mobile devices, notebooks, laptops and desktop computers are issued for use teaching and learning purposes only. Devices must not be used by non-students (ie, friends, family, etc).

The unauthorised duplication of copyrighted computer software violates the law and is contrary to the school's standards of conduct and business practice. The school will comply with all licensing terms and conditions regulating the use of any software it acquires.

2.7 Shared printing

Care must be taken when printing sensitive or confidential material to a shared printer that is not controlled by a student ID, login or print account system. Most printers support the use of password protection and secure print.

2.8 Information security threats

All users are responsible for the security of information that is owned by or entrusted to the school. All actual or suspected security weaknesses must be reported immediately to the Service Desk.

The school has built security features and controls into its email system, network and computers that can detect viruses and malware, but it can never protect from every threat. Students must be confident they can recognise a fraudulent email (eg, phishing attacks) or links and websites. Students must also treat with caution external USB, hard disk and other storage devices where the contents or the source of the device cannot be verified. Users are the first line of defence. Do not click on a link or open a file that is not recognised.

2.9 Use of personal email addresses

Students should access information relating to their studies via their school Email Account. Although not preferred, Users may choose to forward their school Email account to a personal or work email account, so they do not miss out on important information. Users are responsible for all information sent to them via their school email account. If a User chooses to forward their school email account, they are responsible for all information, including attachments, sent to those other email accounts.

2.10 Inappropriate content

Do not download inappropriate material, store it on your computer or on the school network, or include it within email or other communications means. Inappropriate content includes, but is not limited to the following:

- Creation or transmission, or causing the transmission, of any offensive, obscene, or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material, which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the school or a third party or which promotes discrimination based on race, gender, religion or belief, disability, age or sexual orientation.
- Creation or transmission of material with the intent to defraud or which is likely to deceive a third party, or which advocates or promotes any unlawful act.
- Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others. Unsolicited or bulk email (spam), forged addresses, or use of mailing lists other than for legitimate purposes related to the school's activities.
- Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.
- Material that brings the school into disrepute.

- Deliberate unauthorised access to networked facilities or services or attempts to circumvent school security systems.
- Pursuance of commercial activities for personal gain.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
- Wasting employees' effort or time unnecessarily on IT management.
- Corrupting or destroying other users' data.
- Violating the privacy of other users.
- Disrupting the work of other users.
- Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
- Continuing to use an item of networking software or hardware after a request that use should cease because it is disrupting the correct functioning of the network.
- Other misuse of network resources, such as the introduction of computer viruses, malware, or other harmful software.
- Any breach of industry good practice that is likely to damage the reputation of any connected external network, eg, JANET or AAR Net, will also be regarded as unacceptable use of the school Network.
- Introduce data-interception, password-detecting or similar software or devices to the school's Network

2.11 Monitoring

The school reserves the right to regularly audit User activity and IT systems to ensure compliance with this and other Company policies. Our tools provide us with the information to monitor your physical location; however, we only review this information when required to recover lost devices or investigate Information Security incidents. Access to the school's IT systems is provided on condition that users consent to monitoring in accordance with policy. Your use of school IT systems constitutes your consent to the monitoring.

2.12 Personal devices (BYOD) – restrictions whilst on the school network

To protect the school's IT systems, safeguard students, and ensure responsible digital use, the following restrictions apply when connecting personal devices (eg, laptops, tablets, smartphones) to the school network:

- **VPNs and proxy services –** use of Virtual Private Networks (VPNs), proxy services, or any other methods to conceal online activity or bypass the school's network filters is strictly prohibited.
- **Hotspot / tethering –** personal hotspots or tethering to bypass the school's Wi-Fi are not allowed on school premises.
- **Network disruption** – personal devices must not be used in ways that could disrupt or overload the school network (eg, running servers, network scans, or denial-of-service activities).

- **File sharing and torrenting** – peer-to-peer (P2P) file sharing, torrenting, or downloading copyrighted material without permission is forbidden.
- **Unapproved software and apps** – installation or use of unauthorised applications (including hacking tools, anonymisers, or malware testing software) is not permitted.
- **Security compliance** – personal devices must have up-to-date antivirus software, security patches, and device lock/passwords enabled before accessing the school network.
- **Inappropriate content** – accessing or distributing material that is illegal, offensive, or inappropriate for an educational environment is prohibited.
- **Personal streaming and gaming** – excessive use of personal devices for non-educational purposes (eg, streaming, gaming, or social media) that impacts network performance is not permitted during school hours.

Further guidance and requirements are outlined in the school's dedicated BYOD policy.

2.13 Use of generative AI tools

Students may only use AI tools that are approved and provided by the school. At d'Overbroeck's, the approved tool is Copilot.

Students must not:

- use AI to access, create, or share inappropriate or harmful content;
- attempt to use AI to bypass school filters or monitoring systems;
- enter personal information (their own or others') into AI systems;
- present AI-generated work as entirely their own without following school rules on academic honesty.

Students must remember that AI outputs may be incorrect, biased or unsafe and therefore must use them with care and in line with school guidance.

Any concerns about AI use or harmful AI content must be reported immediately to a member of staff.

Misuse of AI will be treated as a serious breach of this Acceptable Use policy and may result in sanctions under the Behaviour policy.

3. Associated policies

Associated policies available from the school website or from the school office on request:

- Behaviour, rules, rewards and sanctions policy
- Bring your own device (BYOD) policy for staff and students
- Data protection policy
- E-safety policy

Acceptable Use of IT Equipment at School

Consent Form

Student agreement

I have read, understood and agree to abide by the rules stated in the 'Acceptable use of IT equipment policy – students'.

I understand the consequences if I do not.

Student name: ____ Year Group: ___________

Signed: ____ Date: ________________

Parent/Guardian consent

I have read and understood the school rules for acceptable use, and I give permission for my son/daughter to access the IT resources at d'Overbroeck's. I understand that the school will take reasonable precautions to ensure that the content accessed through the internet is appropriate, but I accept that the school cannot be held responsible for any inappropriate material that is obtained through the internet.

Student name: ____

Parent /Guardian Name: ____

Signed: ____ Date: ________________

Please return this to d'Overbroeck's as either a hard copy or a scanned copy.