DULWICH COLLEGE
FOUNDED 1619

ICT ACCEPTABLE USE POLICY (PUPILS)

The College provides a computing network which allows a range of devices to connect. The aims of this policy are to:

- to help pupils take responsibility for their own safe and responsible use of technology;
- to minimise the risk of harm to the assets and reputation of the College.

This policy:

- sets out the way in which devices should be used by pupils;
- includes guidelines for the safe and responsible use of the network and the internet; and
- identifies those activities which constitute an abuse of the College's ICT facilities.

The College monitors the use of its computer system including College e-mail accounts, network server storage and cloud storage as well as internet access. The College has the right to deny access to its computer system if this policy is not adhered to.

For the purposes of this policy:

- references to the College's computer system includes any electronic device, equipment, facility, program, resource or system provided by Dulwich College for pupils and/or staff to use; and
- electronic computing equipment will be referred to as "devices" and includes laptops, PCs, tablets, notepads, iPads, iPods, mobile phones, smart watches, headphones and digital cameras.

The policy applies to the whole College including DUCKS and parents are encouraged to read this policy with their child.

The policy applies to pupils using or accessing the College's technology (including College devices) whether or off College premises or using their own or others' technology in a way which affects the welfare of individual(s) within or outside the College community or which brings the College into disrepute.

Breach of this policy may result in disciplinary action (including fixed term or permanent exclusion from the College).

1. General Rules

The general rules below apply:

- when pupils are using devices (whether at the College or elsewhere) that have been provided or made available to them by the College;

- when pupils are using their own devices at the College or otherwise whilst under the supervision of the College (whether or not they are using the College's Wi-Fi); and
- otherwise when the use of ICT would affect the welfare of individual(s) within or outside the College community or which brings the College into disrepute

Pupils must:

a) only access authorised areas of the College network;

d) follow the College's Code of Conduct at all times. Accordingly, pupils must not send or post electronic communications (including on email/Teams, social networking sites, blogs, X (formally known as Twitter), Facebook, Instagram etc.) which are offensive, bullying, defamatory, in breach of any of the College Polices or bring the College into disrepute;

c) only store and access appropriate and legal material;

d) set passwords in accordance guidance from the College and change any password immediately if you think it has been compromised at any time;

e) only engage in lawful activities when using the College's computer network or facilities; and

f) respect the privacy of others and not share photos, videos, contact details or other personal information about members of the College without their express consent (even internally within the College).

Pupils should not:

a) upload or download pirated software, music or videos;

b) breach another person's copyright or other intellectual property rights;

c) log on to another user's account;

d) change the log-in or security settings on any College computer;

e) use the College's computer systems (including WIFI) or equipment to access, view or download pornographic or otherwise offensive material;

f) share their username(s) and password(s) with anyone else;

g) try to circumvent the College's filtering systems or other security measures installed on the College's systems (e.g. by use of VPN proxy services);

h) attempt to spread viruses;

i) run any hacking, encryption or other system tools;

j) access or share content that is illegal or likely to offend other members of the College community e.g. that is discriminatory;

k) use artificial intelligence (AI) in the production of any work or College related activity in accordance with the Use of Artificial Intelligence Policy; or

k) attach any servers to the College network or share local drives, folders or files across the network.

Pupils must remember that they are responsible for all data that exists in their file storage areas (including cloud storage), emails and on personal devices. The Computer Services Department has access to this data.

Boarders should read the Guidelines for Boarders in **the Appendix** to this Policy.

2. Use of College Devices

The College provides devices which are primarily available for educational use during lessons.

In addition to the rules in Part 1 above, pupils should not:

a) physically tamper with College equipment e.g. disconnect equipment from the network, remove the mouse/keyboard/monitor etc. or attempt to repair equipment;

b) upload, download, install or attempt to run any software or download material from any external storage device that has not been approved by Computer Services;

c) alter the settings of the College equipment or make other changes which render the equipment unusable by others; or

d) purchase goods or services over the internet using the College's computer network or facilities.

3. Use of Pupils' Own Devices

Pupils should:

a) only attach their own personal devices by using wireless networking or specially provided network ports (e.g. the network points in the Boarding Houses);

b) ensure that their devices are properly protected from viruses;

c) not run file sharing devices (e.g. personal servers) on the College network;

d) not plug devices directly into any network switch, hub or router;

e) not detach from the network any equipment to make way for a personal device;

f) ensure that they have a licence for all software installed on their devices; and

g) only use their device during a lesson with the teacher's permission.

4. Internet Safety

The College's access to the internet has a filtered service. Internet sites that pupils visit or attempt to visit are logged and reviewed on a regular basis by the Assistant Head Safeguarding to identify patterns of access which cause concern. The Deputy Master Pastoral & Co-Curricular is notified when there are cases which need further investigation.

When using the internet pupils should:

a) only access appropriate sites;

b) immediately tell an adult if they see or read anything they are uncomfortable with;

c) never give out personal information about themselves or others (including passwords) and inform a member of staff if they are concerned they have shared information they should not have;

d) never arrange to meet anyone they don't know;

e) never open e-mails sent by someone they don't know;

f) only access or share other people's files or pictures with their permission;

g) carefully consider the use of any website or application with the capability of identifying the user's location (as the use of location services can represent a risk to pupil's personal safety); and

g) not download copyrighted materials which have not been paid for (including music and videos).

5. Use of Email and other Online Communications (e.g. social media and Microsoft Teams)

Pupils should remember that even when an email/electronic message or something that has been downloaded has been deleted, it can still be traced on the system.

Pupils should:

a) use College email/Teams as the only means(s) of electronic communication with staff; communication either from a personal email account or to a members of staff's personal email address is not permitted.

b) treat emails in the same way as any other form of written communication and not include anything in a message which is not appropriate to be published generally or would be considered inappropriate.

c) remember that anything that is posted online needs to be considered very carefully and pupils should only post messages or images they would be happy for a parent or teacher to see.

Pupils should not:

a) make comments about individuals or the College online; this could cause offence.

b) Use AI to generate images of other people, indecent or otherwise.

6. Monitoring and Access

The College monitors College email and internet usage (including through the College Wi-Fi) and both web history and emailed accounts may be accessed where necessary for a lawful purpose (including serious conduct or welfare concerns, extremism and protection of others). Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances.

7. Related Policies

Pupils should never access or use the College's computer system, or College's devices, or ICT generally in a way that breaches any of the College's policies including:

- Code of Conduct
- Mobile Phones and Wearable Device Policy
- any of the Anti-Bullying Policies
- any of the Behaviour Policies
- Use of Generative Artificial Intelligence Policy

9. Disciplinary Action

Misuse of a College device may result in that device being withdrawn on a temporary or permanent basis.

As stated above, breach of this policy may result in disciplinary action (including fixed term or permanent exclusion from the College).

Policy Owner:	Deputy Master Academic
Last Reviewed:	September 2026
Date of Next Review:	Academic Year 2026-27

Appendix – Guidance for Boarders

The College takes the importance of responsible use of technology in the boarding houses seriously.

The boarding houses are Wi-Fi enabled and each study room has an Ethernet connection to allow laptops and PCs to be connected to the College network.

Pupils are allowed mobile devices in their rooms which can connect to the internet (subject to the rules set out below)..

Printing facilities are also made available to the pupils.

The College expects pupils to comply with the following guidelines with respect to the use of electronic equipment:

1. The ICT Acceptable Use Policy (Pupils) must be observed and pupils who have internet enabled devices must use them safely and within the guidelines stated in that Policy including this Appendix.

2. In accordance with the Copyrights Design and Patents Act (1988) all software installed must be legally licensed for use on that machine and all data (music, videos etc) must be legally acquired.

3. Pupils are expected to protect their machine from viruses and malware and have in place proper procedures for the backup of files which are not on the College system.

4. No pornographic or otherwise offensive or unsuitable material may be stored, downloaded or viewed on electronic devices.

5. The College does not accept responsibility for the security of pupils' equipment and parents should ensure that they have made satisfactory insurance arrangements.

6. Maintenance or repairs are entirely the responsibility of the parents and adequate provision for technical support should be made.

7. The College reserves the right to ensure that these guidelines are being complied with, including by carrying out a physical inspection of equipment and examination of the contents of the hard disk and other storage media, including retrieving internet logs.

8. Machines connected to the College network access the Internet through a firewall and content is filtered. No attempt should be made to bypass this filter (e.g. by using a VPN proxy server). Requests for blocked sites to be made available should be directed in the first instance to Housemasters.

9. Any suspicious behaviour the pupils encounter on any electronic device must be reported to their Housemaster immediately.

10. Pupils are encouraged to use mobile devices responsibly and aim to do so through a policy of education.

11. Using machines for non-academic purposes must not interfere with the routine of the House, most importantly 'lights out'. Housemasters are conscious of their duty of care towards the pupils with regard to adequate sleep, and excessive use of mobile devices can be a cause for concern. Housemasters will exercise their duty of care when necessary in this regard and reserve the right to remove devices from pupils for the sake of their wellbeing and sleep hygiene.

The following rules apply to the use of devices (including mobile phones) by boarders:

Years 9-11

- All devices are taken in at night (mobile phones, laptops, tablets etc.) charged and returned before breakfast the following morning.
- Using mobile phones for non-academic purposes must not interfere with the routine of the House.
- Normal school rules apply from 8am to 4pm.
- Mobile phones are permitted in the Boarding House after school but there are restrictions on games allowed and social media use through the College firewalls.
- No mobile phones are permitted during prep time (1 hour each evening) and mobile phones not allowed in the dining hall at breakfast or supper.

Years 12-13

- Mobile phones and other devices are allowed overnight but gaming/tiredness will be monitored by Boarding Housemasters and Form Tutors who are conscious of their duty of care towards the pupils with regard to adequate sleep; excessive use of mobile devices can be a cause for concern. Housemasters will exercise their duty of care when necessary in this regard and reserve the right to remove devices from pupils for the sake of their wellbeing and sleep hygiene.
- Using mobile phones for non-academic purposes must not interfere with the routine of the House, most importantly 'lights out'.
- Normal school rules apply from 8am to 4pm.
- Wifi goes off in the Boarding Houses at 11.30pm weekdays and 12.30am weekends.