BRADFIELD COLLEGE

IT Acceptable Use Policy

Document Control	
Document title:	IT Acceptable Use Policy
Author:	Mr Trevor James Benstock
Version number:	1.8
Document status:	Approved by Andy Logan
Effective date:	September 2024
Date of next full review:	September 2025
Documentation Location	College website / Firefly

Version	**Author**	**Date**	**Changes**
1.7	TJB Updated AUP	26/09/2021 Status: Review complete	Updated technical language used. Removed ambiguous reference to College room search policy, included specifics. Updated guidelines.
1.8	PL, SRD and DJB Updated AUP	26/6/2024	Updated recommended use of OneDrive for pupils and password advice. Included mended reference to Mobile Device Policy, AI and logging.

BRADFIELD COLLEGE

IT Acceptable Use Policy

Internet access, **computers** and **laptops** are available primarily to support academic work, research and study. In instances where an individual's use of IT is deemed irresponsible or inappropriate, access to the network will be removed for a period of time while the matter is investigated. Please note that the College firewall retains records of the websites that you access. The use of Virtual Private Networks (VPNs) is banned at the College. VPNs allow users to bypass the College's filtering and monitoring systems. If a user is found to be using a VPN the pupil will be sanctioned accordingly. Appropriate online use is also covered in the Online Safety Policy.

Mobile Phones are permitted at Bradfield primarily to support pupils' family life and the effective operation of the school, this is a privilege and not a right. Pupil access to their mobile phones is covered in the Mobile Device policy. You should use your mobile phone responsibly. In instances where an individual's use of a mobile phone is judged irresponsible, his/her phone may be confiscated while the matter is investigated. Repeated irresponsible use of a mobile phone will be reported to and dealt with by the Second Master or the Deputy Head Pastoral.

You should be aware that computer/mobile phone memory (including any external storage media that a pupil brings into the College) will be subject to the provisions of College policy "Searching of Pupils, their Property or their Rooms", which can be found in Appendix C7 of the Behaviour Policy. As such, on the strength of a justifiable *prima facie* cause, investigating staff may review files and messages.

Material downloaded in the home or from outside of the College, posted on-line from or transmitted to a device from a remote location, can impact significantly upon the life of staff and pupils at College. It is expected that, at home as much as at school, your use of IT will comply with the College's ethos, accord with the College Rules and honour the acceptable-use policy.

The ethos at Bradfield is borne out of care, consideration and respect for yourself and others therefore certain activities are strictly prohibited when using IT, examples include:

- Using IT to in some way harass, insult, embarrass or in any way intimidate or attack others.
- Using IT to view, send or receive obscene or offensive images/messages including those generated by AI.
- Using IT to gain access to another person's data. E.g. email, user account
- Using another person's device or personal data without their consent
- Using IT to imitate somebody else on any platform, including social media
- Using accounts or passwords of others when making use of IT in any form
- Using IT to plagiarise material or otherwise violate laws of copyright
- Using IT to view, send, receive pirated material or access the 'dark web'.
- Deliberately damaging or corrupting computers, systems or network peripherals
- Installing, distributing or promoting malicious software or website(s)

BRADFIELD COLLEGE

IT Guidelines

1. Keep your password secure. Do not tell anyone else what it is. Passwords should be set up as three random words (as per the advice given by the National Cyber Security Centre). The College also recommends use of Edge Password Manager protected by a secure password and two-factor authentication.
2. A secure network is provided to the benefit of all. Respect the safeguards in place and do not attempt to bypass filters or user permissions. Do not use VPN tunnels, Proxy Servers or non-Bradfield College Internet Services to access on-line material. If a legitimate website is blocked please ask a member of staff to contact IT Services on your behalf.
3. If you are using a computer and you find something unpleasant, obscene or offensive please inform IT Services immediately. Be aware that any activity performed that utilises the College network and system, is logged.
4. Never give out personal information (including photos/videos) to anyone you do not know.
5. Keep your personal data (including social media profiles) private.
6. Save your work regularly and backup all of your important files, particularly any work you store locally to your own device(s). Files should be saved on your Bradfield College OneDrive to ensure it is backed up, safe and secure.
7. Avoid wasting file server space. Please delete any out of date or unwanted files. The College reserves the right to delete non-education related material from the network. We strongly advise personal files be stored on non-networked personal devices or your personal cloud drives.
8. Think before you print, save paper whenever possible. Print job log files are retained.
9. When using a College device remember to close down and log off your session correctly.
10. Copying software is illegal. Please respect the rights of authors and do not copy from the school network or any other source. Those who do are liable to prosecution.
11. If you encounter an IT problem or require assistance please log a ticket with the IT Services department: helpdesk@bradfieldcollege.org.uk

July 2024