BRADFIELD COLLEGE

Online Safety Policy

Document Control	
Document title:	Online Safety policy
Author:	Sarah Davies, Designated Safeguarding Lead
Document status:	Approved
Approved by:	Pastoral Committee
Effective Date:	November 2024
Version number:	2.5
Date of next full review:	September 2025

Version	Author	Date	Changes
1.0	T Benstock	Feb 2018	Update on IT security
2.0	S Davies	Sept 2019	Reviewed
2.1	S Davies	Lent 2020	Reviewed
2.2	S Davies	May 2021	Reviewed by pupil Digital Leaders and e-safety committee. Some additions made for clarity and fullness.
2.3	S Davies	July 2022	Reviewed and additions made in line with KCSIE 2022 and new NMS
2.4	S Davies	October 2023	Reviewed and additions made re filtering and monitoring, and the role of the DSL in online safety in line with KCSIE 2023. Rename of policy to "Online Safety Policy" for consistency with KCSIE nomenclature.

			Addition of further detail on online safety in the curriculum and engagement with pupils and staff. Addition of useful resources and links.
2.5	S Davies	October 2024	Reviewed section "What is online safety" – inclusion of AI and deepfakes.

BRADFIELD COLLEGE

Online Safety Policy

Reviewed October 2024

Contents

Online Safety Policy

Safeguarding Mission Statement

Bradfield College is committed to providing a caring, friendly and safe environment for all its pupils so they can learn in a relaxed and secure atmosphere. The College takes seriously its responsibility to protect and safeguard its pupils. Ours is a TALKING school. This means that anyone who has worries about a pupil in the College ought to talk about it. Telling is not "dobbing in" or "grassing".

STATEMENT OF PRINCIPLES

This policy aims to ensure that all pupils and staff at Bradfield College use technology in such a way as to protect and promote the welfare of all members of the community, and of the pupils in particular. The whole ethos of Bradfield College aims to create amongst all who work or study here mutual respect and understanding of the needs of others.

This policy will be made available to staff, pupils and parents via the Bradfield Website and in hard copy from the Pastoral Office. Because of the rapidity of on-going developments in young people's on-line experience, this Online Safety policy is kept under on-going review.

POLICY REACH

The policy for Online Safety applies to all pupils, College employees, volunteers working at the College, and to agents employed indirectly by the College. It also applies to members of Council, the College governing body. It is designed to sit alongside, and should be read in conjunction with, other related College policies such as the Child Protection and Safeguarding Policy, the Anti-Bullying Policy, the Behaviour Policy, and the Acceptable Use Policy.

WHAT IS ONLINE SAFETY?

Whilst the Internet and associated technologies are invaluable tools for enriching learning, several risks accompany their use, including:

- **Cyberbullying**: Harmful messages or images sent through email, social media, and messaging platforms such as WhatsApp, Snapchat, or Instagram. (cf Anti-Bullying Policy Sections 3.7-3.8).
- **Deepfakes and AI Misuse**: The manipulation of images or videos to create deceptive content (e.g., deepfakes) and other AI-generated media that may distort reality or harm individuals.
- **Exposure to Inappropriate Material**: Potential for encountering unsuitable or adult content.
- **Sexting and Sextortion**: Sharing explicit images (Youth Produced Sexual Images) and coercive sextortion.
- **Illegal Activities**: Engaging in behaviours like hacking, spamming, accessing pirated media, or easily accessible gambling platforms.
- **Inappropriate Group Content**: Content and titles of group chats (e.g., on WhatsApp) that may promote harm or distress.
- **Internet Obsession**: Overuse of platforms like YouTube, social media, forums, or gaming sites, leading to reduced wellbeing.
- **Predatory Risks**: Vulnerability to sexual predators posing as peers.
- **Malware and Viruses**: Accidental downloads of harmful software such as viruses, Trojans, or trackers that may compromise devices and data.
- **Proxy or VPN Use**: Intentional bypassing of filtering services via proxies or VPNs to access restricted content.

- **Fake Account Creation**: Unauthorised creation of fake accounts that mimic the College or its students and staff, including identity theft for offensive content.
- **Password Security**: Sharing passwords or other private account details is prohibited. Suspected breaches should be reported to IT Services immediately, and passwords should be updated.

Bradfield College will assume responsibility for protecting all members of our community from such dangers by technical means (such as internet filtering and monitoring) and by educational means designed to ensure that pupils and staff understand how to operate safely online.

1. ONLINE SAFETY RESPONSIBILITIES AT BRADFIELD COLLEGE (CF ANTI-BULLYING POLICY APPENDIX B3)

1.1 All Staff

Online safety will be the concern of all staff at the College. All adults acting *in loco parentis* and who come into contact with children have a 'duty of care' for them, and this duty of care extends to all matters relating to the use of technology. All staff who work at Bradfield College will receive regular training in their child protection responsibilities, and all teaching staff will receive specific training in matters of online safety, including use of the internet, filtering and monitoring, and cyberbullying. In addition those staff who work in boarding houses will receive guidance and training with regard to the potential for cyberbullying, hoaxes, harmful online challenges, and all forms of harassment within a boarding environment. The College also pays particular attention to approach to harmful online content and how boarders' devices are managed in terms of devices brought into the boarding environment, and any harmful content that may already be downloaded on to it, and the opportunity to download harmful content via 3,4 and 5G or VPNs that will bypass the school's filtering and monitoring systems.

In particular, all staff will have a clear understanding of online safety issues, know how to report online safety concerns, abide by the staff AUP (Acceptable Use Policy), give due concern to the reputation of the College and its members before they post online, contribute to a whistleblowing culture where they have any suspicion or concern, and never befriend current pupils or recent leavers on social media themselves.

The school will:

- Provide and discuss the Online Safety Policy and staff Acceptable Use Agreement with all members of staff as part of induction
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will include an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Make staff aware that school systems are monitored and activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

1.2 All Pupils

All pupils at the College will contribute to the ethos of the College by showing respect for and understanding of the needs of others. In addition, they will comply with the AUP (Acceptable Use Policy) each time they login to the Bradfield network. Furthermore, they will participate in and gain an understanding of online safety matters from Wellbeing provision, assemblies, lectures and informally in houses. Ours is a talking school, and pupils will report any concerns they may have regarding online safety issues including within the boarding environment. All pupils will know how to report online safety concerns or problems via Firefly, or by telling a trusted member of the College Staff, a Prefect or one of the pupil Digital Leaders.

1.3 Online Safety Committee

The Online Safety Committee, reporting to the Pastoral Committee, will provide a consultative group with wide representation from the school community. It will have oversight of issues regarding online safety (including the College's education of pupils, staff and parents), and responsibility for monitoring policy in the light of emerging technologies. It is chaired by the staff Online Safety Co-ordinator who also runs the pupil Digital Leaders Programme "WebForum" and Pupil Online Safety Committee.

1.4 Pupil Online Safety Committee

The Pupil Online Safety Committee will report to the Online Safety Committee. It will be made up of interested pupils from across the spectrum of the pupil body. Its purpose will include the regular review of current trends in technology including AI, advising the Online Safety Committee on pupil use of new technologies, and informing the College staff and pupils on trends and issues through termly Assemblies. It will also contribute where possible to outreach online safety programmes eg visiting local primary and prep schools to discuss and promote online safety.

1.5 Director of IT Services

The Director of IT Services will have overall responsibility for ensuring the best technological solutions are in place to ensure online safety (to include filtering and monitoring software), whilst still enabling the pupils to use the Internet effectively in their learning. They will also ensure that all information captured using these systems is securely stored, and accessible to appropriate members of staff. They will assist with the development of the online safety education programme for pupils and staff, and they will sit on the Online Safety Committee to advise on online safety matters and review online safety policy.

1.6 Wellbeing and Online Safety in the Curriculum and engagement with pupils

The Head of Wellbeing will be responsible for delivering online safety instruction in the curriculum and for the Wellbeing lecture programme that includes talks on online safety related matters. They will also sit on the Online Safety Committee.

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety across the curriculum, including the Wellbeing, Relationships

and Sex Education programmes of study, covering use both at school and home
- Reinforcing online safety messages whenever technology or the internet is in use
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Teaching pupils to be critically aware of what they see online and shown how to validate information before accepting its accuracy
- Teaching pupils to respect and adhere to principles of academic integrity. This will include understanding the importance of producing their own independent work, being transparent and honest about any use of source material or generative applications, respecting copyright and using appropriate referencing conventions
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

1.7 DSL and Deputy DSLs

The DSL (Designated Safeguarding Lead) will have both an operational and strategic duty to act as the lead person in matters of Child Protection and Safeguarding and online safety.

The Deputy DSLs will work with the DSL to ensure that policies, protocols and records regarding Child Protection and Safeguarding are up-to-date. Full details of their roles can be found in the Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL):

- Takes lead responsibility for online safety (including understanding the filtering and monitoring processes and systems in place)
- Works with the Online Safety Co-ordinator to promote an awareness of and commitment to online safety throughout the school community
- Works with the Deputy Head Pastoral and Second Master in maintaining the College Bullying Register, which records all instances of Cyber-bullying.
- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Monitors pupil internet usage, taking action where required
- Maintains the online safety incident log and record of actions taken, and reviews the log periodically to identify gaps and trends
- Reports regularly to the Governors, Head and SMT on the incident log, internet monitoring, current issues, developments in legislation etc.

2. THE COLLEGE RESPONSE TO BREACHES OF ONLINE SAFETY (CF ANTI-BULLYING POLICY APPENDIX B3)

Bradfield College will use its existing procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a pupil. (These may include breaches of filtering or the AUP, illegal or inappropriate use, cyberbullying, or the use of ICT to groom a child or to perpetrate abuse.)

The College is determined to combat cyber-bullying and recognises that the effects of online bullying can often be amplified by the potential reach of material posted online, the greater scope for bringing the College into disrepute, and the additional anxieties that can be caused by the abuse of online anonymity. Pupils will be held responsible for material they have posted when absent from the College premises. Sanctions can include the confiscation of mobile phones or personal computers, gating, suspension and expulsion. Pupils are briefed on the College Online Safety Policy in regular assemblies and within the Wellbeing curriculum.

This policy needs to be read in conjunction with the College's Mobile Devices Policy.

Useful links and sources of advice

Guidance and resources

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Harmful online challenges and online hoaxes (DfE)
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Self-generated child sexual abuse (IWF)
- Meeting digital and technology standards in schools and colleges March 2022 (DfE)
- Generative artificial intelligence in education (DfE)

National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Telephone helpline: 0844 381 4772

This policy is subject to ongoing review.
Last reviewed: October 2024
SRD