

BRADFIELD COLLEGE

Online Safety Policy

Document Control

Document title	Online Safety Policy
Author	Sarah Davies, Designated Safeguarding Lead
Document status	Live, pending sign off at Pastoral Committee
Approved by	Pastoral Committee
Effective date	September 2026
Version number	3.2
Date of next full review	September 2027
Documentation location	Website / About Us / Policies and Staff Policy Area

Version history

Version	Author	Date	Changes
2.6	S Davies	September 2025	Reviewed and amended to include Securly system and KCSIE 2025 references, including AI and misinformation.
3.0 draft	S Davies	August 2026	Substantial redraft for KCSIE 2026, statutory Mobile Phones in Schools guidance, updated filtering and monitoring expectations, AI/deepfake risks, and alignment with Mobile Phone Policy V8.
3.1 draft	S Davies	August 2026	Consultant review integrated: strengthened governance and cyber-security oversight, service-provider liaison, Prevent-linked review, smart/camera-enabled wearables, pupil-image security, and additional technical/cyber-risk reporting.
3.2 draft	S Davies	August 2026	Added explicit College expectations on recording, live transcription and

			AI/automated note-taking
--	--	--	--------------------------

Summary of substantive changes

Area	Change made
Statutory framework	Updated to refer to KCSIE 2026, statutory Mobile Phones in Schools guidance, DfE filtering and monitoring standards, UKCIS sharing nudes/semi-nudes guidance, Prevent and DfE digital and technology standards.
Mobile devices	Aligned with Mobile Phone Policy V8: mobile-phone-free by default; Lower College managed device plus one; restricted Sixth Form access; no VPNs, eSIMs, fake phones, MiFi or other circumvention.
Filtering and monitoring	Added clear ownership, annual effectiveness review, regular checks, action tracking and escalation routes involving DSL, DDSL, IT and SLT/governance.
AI/deepfakes	Strengthened explicit reference to generative AI, deepfakes, synthetic sexual imagery, impersonation, misinformation and AI-assisted bullying/abuse.
Incident response	Added clearer process for online safety incidents, including safeguarding triage, evidence preservation, police/children's social care escalation and prohibition on staff routinely viewing or forwarding nudes/semi-nudes.
Staff conduct	Added staff mobile phone expectations and professional online conduct guidance.
Curriculum/parents	Strengthened pupil education and parent engagement, especially around mobile-phone-free expectations, AI, sexual imagery, online misogyny, radicalisation, gambling and wellbeing.
Consultant review	Integrated consultant additions on governor/SLT scrutiny, cyber security and provider liaison, Prevent-linked annual review, smart glasses/camera-enabled devices, image security, and cyber-risk reporting.
Recording and transcription	Added explicit prohibition on audio/video recording, live transcription and AI/automated note-taking of lessons, meetings, forums, calls or conversations without explicit prior permission of all parties, with tightly defined authorised exceptions.

Online Safety Policy

Safeguarding Mission Statement

Bradfield College is committed to providing a caring, friendly and safe environment in which all pupils can learn, live and flourish. The College takes seriously its responsibility to protect and safeguard pupils. Ours is a talking school: anyone who has worries about a pupil should talk about it. Telling is not dobbing in or grassing. When pupils talk to us, we listen and act appropriately and effectively on their concerns and suggestions.

Online safety is part of safeguarding. It is not a separate technical matter: it affects pupils' welfare, behaviour, mental health, relationships, learning, boarding life and sense of belonging.

1. Statement of principles

This policy sets out how Bradfield College helps pupils and staff to use technology safely, respectfully and responsibly. It aims to protect and promote the welfare of all members of the College community, and pupils in particular.

The College recognises both the educational value of technology and the risks associated with online activity. It seeks to enable confident, creative and purposeful use of technology while reducing risks of harm, abuse, distraction, disruption, addiction, bullying, exploitation, radicalisation and unsafe or unlawful behaviour.

This policy is kept under ongoing review because pupils' digital lives and the technologies available to them change rapidly.

2. Policy reach

This policy applies to all pupils, staff, volunteers, Council members, contractors, visitors and agents employed directly or indirectly by the College. It applies to use of College systems, College-managed devices, personal devices, mobile phones, smart watches, tablets, laptops, wearable technology, online accounts, cloud storage, apps, social media, gaming, messaging platforms and any internet-enabled technology used on or off the College site where the conduct affects the welfare, reputation or safety of the College community.

It should be read alongside the Child Protection and Safeguarding Policy, Mobile Phone Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, Staff Code of Conduct, Data Protection Policy, IT Security/Cyber Security procedures, Prevent risk assessment and relevant boarding policies.

3. Statutory and guidance framework

This policy has regard to the following statutory and non-statutory guidance and standards:

- Keeping Children Safe in Education 2026, including expectations on online safety, filtering and monitoring, mobile phones, child-on-child abuse, sharing nudes and semi-nudes, and safeguarding risks linked to generative AI and deepfakes.

- Mobile Phones in Schools: statutory guidance, applicable from 1 September 2026, including the expectation that schools are mobile-phone-free by default during the school day and that exceptions are carefully defined and consistently managed.
- DfE Filtering and Monitoring Standards and wider Meeting Digital and Technology Standards in Schools and Colleges.
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- DfE guidance on Searching, Screening and Confiscation, Behaviour in Schools, Prevent, Relationships Education/RSE and Health Education, and Teaching Online Safety in School.
- Boarding Schools: National Minimum Standards, including the expectation that boarders are supervised effectively and that staff know, or can establish, their whereabouts.

4. What is online safety?

Online safety describes the College's approach to helping pupils and staff benefit from technology while recognising, preventing and responding to online risks. The College considers online risks using the four commonly recognised areas of content, contact, conduct and commerce.

4.1 Content risks

- Exposure to harmful, inappropriate, violent, degrading, racist, misogynistic, homophobic, pornographic, extremist or age-inappropriate material.
- Misinformation, disinformation, conspiracy material, harmful online challenges and online hoaxes.
- AI-generated or manipulated content, including deepfakes and digitally altered images or videos.

4.2 Contact risks

- Grooming, sexual exploitation, criminal exploitation, coercion, sextortion and predatory contact by adults or peers.
- Contact with unknown individuals through social media, gaming, messaging platforms, livestreaming, forums or anonymous apps.
- Radicalisation, recruitment, coercive online communities and online misogyny/manosphere influences.

4.3 Conduct risks

- Cyberbullying, harassment, humiliation, exclusion, abusive group chats, misuse of images, impersonation and fake accounts.
- Making, requesting, possessing or sharing nudes and semi-nudes, including AI-generated or digitally manipulated sexual imagery.
- Unsafe or unlawful use of technology, including hacking, sharing passwords, unauthorised access to accounts, recording or photographing others without permission, and use of technology to facilitate child-on-child abuse.
- Recording, transcribing or using live transcription, automated note-taking or AI transcription tools to capture a lesson, meeting, forum, telephone/video call, conversation or other College interaction without the explicit prior permission of all parties whose contributions may be captured.
- Overuse of screens, internet obsession, sleep disruption, social withdrawal and reduced wellbeing.

4.4 Commerce and technical risks

- Gambling, loot boxes, scams, fraud, phishing, identity theft, malicious links, malware, spyware, trackers and viruses.
- Cyber-attacks and unauthorised access may originate from within or outside the College; pupils are reminded that attempts to compromise College systems are prohibited and will be investigated.
- Downloads or activity involving malware, viruses, Trojans, trackers or other harmful software - whether accidental, deliberate or arising from an external scam - must be reported to IT Services immediately.
- Attempts to bypass College systems, filtering or monitoring by using VPNs, proxies, fake phones, additional devices, eSIMs, MiFi, dongles, embedded network cards, mobile data, tethering or another pupil's login details. These are Notifiable Offences and will result in a significant sanction.
- Use of unapproved apps or services that create privacy, safeguarding, reputational or data protection risks.

Bradfield College addresses these risks through education, culture, pastoral support, behaviour systems, technical controls, filtering and monitoring, clear mobile-device rules, and proportionate safeguarding responses.

5. Mobile devices and mobile-phone-free expectations

This policy must be read alongside the Mobile Phone Policy. The College's approach is that pupils should be mobile-phone-free by default during the school day. Mobile phones must not be used in lessons, during movement time around the site, at breaks or at lunch unless an explicit exception applies under the Mobile Phone Policy.

Lower College pupils are expected to follow the "managed device plus one" approach set out in the Mobile Phone Policy. Faulkner's, Shell and Fifth Form pupils should only have their College-managed device and one mobile phone. Access to personal mobile phones is restricted by year group and House arrangements. Smart watches are treated as mobile phones.

Sixth Form pupils are granted limited, defined access reflecting their age and independence, but phones should not leave House during the academic day and must not be used visibly around younger pupils or in public school spaces unless expressly permitted.

Reasonable adjustments or individual exceptions may be made for disability, medical need, safeguarding need or other exceptional individual circumstances. These should be agreed and recorded by the relevant HsM, Deputy Head (Pastoral), DSL or medical team as appropriate.

Attempting to bypass College online safety systems is prohibited. This includes use of VPNs, proxies, fake or additional phones, eSIMs, MiFi, dongles, embedded network cards, mobile data/tethering or another person's credentials. Such behaviour will be managed under the Mobile Phone Policy, Behaviour Policy and, where relevant, safeguarding procedures.

6. Roles and responsibilities

6.1 Council and senior leadership

Council and senior leaders are responsible for ensuring that the College has appropriate online safety, filtering and monitoring arrangements in place and that these are reviewed effectively. Online safety, including filtering and monitoring, will be reported to the relevant senior leadership and governance committees at least annually and more frequently where risk or incidents require it.

Council, the relevant senior leader and IT staff will maintain scrutiny of filtering, monitoring and cyber-security arrangements and will liaise with relevant service providers. Council will review the applicable standards and, with IT staff and service providers, consider what more may be required to meet them. A member of SLT will maintain overall responsibility for cyber security and will report through the Headmaster to Council.

6.2 Headmaster, Second Master and Deputy Head (Pastoral)

- Ensure that online safety expectations are embedded in safeguarding, behaviour, pastoral and boarding practice.
- Ensure the Mobile Phone Policy is implemented consistently and that sanctions for breaches are clear, proportionate and recorded.
- Work with the DSL and Director of IT Services to review trends, serious incidents and emerging risks.
- Ensure pupils, parents and staff receive clear communication about online safety and mobile-device expectations.

6.3 Designated Safeguarding Lead and Deputy DSLs

The DSL takes lead responsibility for online safety as part of safeguarding. The DSL will:

- understand the College's filtering and monitoring systems and processes;
- receive and triage online safety concerns where there is a safeguarding element;
- ensure online safety incidents are recorded appropriately and reviewed for patterns and trends;
- monitor Securly and other safeguarding alerts, taking or coordinating action where required;
- ensure staff know how to report online safety concerns and what to do if they encounter suspected nudes or semi-nudes;
- work with IT, the Deputy Head (Pastoral), Head of Wellbeing and Online Safety Co-ordinator to review risk and pupil education;
- report relevant trends and serious concerns to SMT, the Headmaster and governors/Council as appropriate.

6.4 Director of IT Services

The Director of IT Services is responsible for ensuring that technical systems support a safe online environment while enabling effective teaching and learning. This includes filtering, monitoring, cyber security, secure storage of monitoring data, account security, device management, system logs and timely escalation of technical concerns to safeguarding or senior colleagues.

The Director of IT Services will liaise with providers of filtering, monitoring and other relevant IT-security systems, and will ensure that Council/governors are appropriately briefed on, and where appropriate involved in, this liaison.

6.5 Online Safety Committee

The Online Safety Committee reports to the Pastoral Committee and provides a consultative group with representation from safeguarding, IT, pastoral, curriculum, boarding and pupil voice. It reviews emerging technologies, pupil trends, incident patterns, curriculum provision, parent communication and the effectiveness of online safety systems.

6.6 Pupil Online Safety Committee / Digital Leaders

The Pupil Online Safety Committee/Digital Leaders will contribute pupil voice on emerging trends, app use, online pressures, AI, gaming, group chats and peer culture. They may support assemblies, peer education and outreach work, but they are not responsible for managing safeguarding concerns.

6.7 Head of Wellbeing and curriculum leads

The Head of Wellbeing is responsible for ensuring that online safety is addressed through the Wellbeing curriculum and wider educational programme. The curriculum will be age-appropriate, regularly reviewed and responsive to emerging risks.

6.8 All staff

All staff have a responsibility to promote safe, respectful and responsible use of technology. Staff will:

- complete online safety training, including filtering and monitoring, AI/deepfakes, cyberbullying and safeguarding risks in boarding, misuse of smart spectacles/glasses or other camera-enabled wearable technology, and bullying and harassment of any kind;
- report online safety concerns promptly via the College safeguarding procedures;
- avoid using personal mobile phones for personal reasons in front of pupils during the school day, except in emergencies or where there is a legitimate professional need;
- use College systems and devices professionally and in accordance with the Staff Acceptable Use Policy and Staff Code of Conduct;
- never befriend current pupils or recent leavers on personal social media;
- model the Mobile Phone Policy and challenge visible or inappropriate pupil mobile phone use consistently.

6.9 Pupils

Pupils are expected to use technology safely, respectfully and responsibly. They must comply with the Acceptable Use Policy, Mobile Phone Policy and Behaviour Policy, and should report concerns to a trusted adult, House staff, the DSL team, through Firefly/reporting routes, or via other clearly communicated reporting mechanisms.

6.10 Parents and carers

Parents and carers are expected to support the College's online safety and mobile-device expectations. The College will communicate key messages to parents, including mobile-phone-free expectations, safe use of technology, AI/deepfake risks, age-appropriate app use, online sexual imagery, sleep and wellbeing, and how to raise concerns.

7. Filtering and monitoring

Bradfield College uses filtering and monitoring systems to reduce the risk that pupils are exposed to harmful or inappropriate content and to help identify pupils who may be at risk. The College currently uses Securly and other appropriate systems to monitor activity on College systems and managed devices. Senso or equivalent monitoring may also be used where appropriate for particular pupil groups or devices.

Filtering and monitoring are not a substitute for good safeguarding culture, staff vigilance, education or pastoral care. Staff should remain alert to pupil behaviour, disclosures, concerning online activity and attempts to bypass technical controls.

7.1 Responsibilities for filtering and monitoring

- The DSL has safeguarding oversight of filtering and monitoring arrangements and understands the processes and systems in place.
- The Director of IT Services has technical responsibility for the effective operation, maintenance and security of filtering and monitoring systems.
- The Deputy Head (Pastoral), Second Master and relevant senior leaders support behaviour, pastoral and operational responses to breaches or trends.
- Council/senior governance receives assurance that the College's filtering and monitoring arrangements are appropriate and reviewed.

7.2 Review and assurance

The College will review the effectiveness of filtering and monitoring at least annually, and sooner where there are significant changes to technology, pupil risk, systems, staffing, network configuration or safeguarding concerns. This review will involve, as a minimum, the DSL or delegated Deputy DSL, Director of IT Services and a senior leader with responsibility for safeguarding/pastoral care. The review will consider:

- the age and risk profile of pupils, including SEND, mental health, boarding, EAL and other vulnerabilities;
- what is blocked or allowed and whether filtering is age-appropriate and proportionate;
- monitoring alerts, response times, escalation routes and any missed or delayed responses;
- whether systems apply appropriately to College networks, managed devices, guest networks and boarding environments;
- attempts to bypass filtering via VPNs, mobile data, eSIMs, MiFi, proxies or other devices;
- whether staff understand how to report concerns and how filtering/monitoring supports safeguarding;
- action points, ownership and deadlines arising from the review.

The outcome of the annual review and any significant issues will be reported to the relevant senior leadership/governance forum.

8. Education, curriculum and pupil engagement

The College will provide age-appropriate online safety education through Wellbeing, RSE, assemblies, lectures, tutor/House time, academic curriculum opportunities and pupil-led work. Education will address both school and home contexts, and will precede or accompany access to technology.

- safe and respectful communication, kindness, privacy and consent;
- cyberbullying, group chats, image-based abuse and reporting routes;
- making or sharing nudes and semi-nudes, including AI-generated or digitally manipulated images;
- online grooming, exploitation, sextortion and unhealthy relationships;
- online misogyny, radicalisation, extremist content, harmful online challenges and conspiracy material;
- gaming, gambling, loot boxes, financial harms, scams and phishing;
- digital wellbeing, sleep, attention, addiction and healthy boundaries;
- AI literacy, misinformation, academic integrity, plagiarism, copyright and appropriate use of generative AI, including the advantages of safe and purposeful use of AI as well as its risks and dangers;
- how filtering and monitoring work, why VPNs/circumvention are prohibited, and how pupils can seek help without fear.

The needs of pupils who may be more vulnerable online, including pupils with SEND, mental health needs, social isolation, previous safeguarding concerns or other vulnerabilities, will be considered in curriculum planning and pastoral support.

9. Responding to online safety incidents

Bradfield College will respond firmly, fairly, proportionately and with care to online safety incidents.

Responses may involve safeguarding action, pastoral support, behaviour sanctions, parental engagement, technical investigation, police involvement, children's social care, LADO consultation or external agency advice depending on the nature and seriousness of the concern.

9.1 Reporting

Any member of staff who becomes aware of an online safety concern involving a pupil must report it through the College safeguarding procedures. Where there is immediate risk of harm, the DSL or a Deputy DSL should be contacted without delay. Concerns involving staff, volunteers or adults connected to the College must be reported in line with the Child Protection and Safeguarding Policy and low-level concerns/allegations procedures.

9.2 Nudes and semi-nudes

Incidents involving the making, requesting, possession or sharing of nudes or semi-nudes, including AI-generated or digitally manipulated images, must be referred to the DSL or a Deputy DSL. Staff must not routinely view, copy, print, save, forward or share such images. Where an image has been seen accidentally or is unavoidable in order to establish immediate risk, this should be recorded and the DSL should manage next steps in line with UKCIS guidance and the Child Protection and Safeguarding Policy.

9.3 Searching, confiscation and evidence

Where a device may contain evidence of a breach or safeguarding concern, staff should follow the College Behaviour Policy, Mobile Phone Policy and DfE Searching, Screening and Confiscation guidance. Searches or requests to view content should be proportionate, recorded and escalated to the DSL where there is any safeguarding concern. Devices may be confiscated and secured where appropriate. Evidence should be preserved without unnecessary viewing or onward sharing.

9.4 Cyberbullying and child-on-child abuse

Cyberbullying, harassment, image-based abuse, abusive group chats, impersonation, exclusion, misogyny, racism, homophobia, sexual harassment and other online child-on-child abuse will be managed in line with the Anti-Bullying Policy, Behaviour Policy and Child Protection and Safeguarding Policy. The College recognises that online abuse may take place away from College but still affect pupils' safety, wellbeing and education.

9.5 Sanctions and support

Sanctions may include confiscation of devices, mobile phone infringements, gating, loss of device privileges, restrictions on network access, reflective tasks, meetings with parents, suspension or other sanctions under the Behaviour Policy. Sanctions will be applied proportionately, with reasonable adjustments where required, and alongside support where online behaviour suggests addiction, coercion, vulnerability or safeguarding risk.

10. Staff training and professional conduct

All staff will receive online safety training on induction and regular updates thereafter. This will include filtering and monitoring, mobile phone expectations, AI/deepfakes, nudes and semi-nudes, cyberbullying, online sexual abuse, child-on-child abuse, radicalisation, harmful online content, professional boundaries and how to report concerns. Training will also cover the College's expectations on recording, live transcription and AI/automated note-taking, including the requirement for explicit prior permission.

Staff are reminded that activity on College systems may be monitored and traced to individual users. Staff must use College systems and personal social media professionally and must consider the reputation, privacy and welfare of pupils, colleagues and the College before posting online.

11. Boarding context

As a boarding school, the College recognises that online safety extends beyond the formal teaching day. House staff have an important role in supporting healthy routines, sleep hygiene, safe communication, social wellbeing and supervision of devices. Boarding staff should remain alert to risks arising from mobile data, additional devices, VPNs, downloaded content, harmful group chats, nighttime device use and pupils who appear isolated or distressed as a result of online activity.

House routines, device hand-in arrangements, evening restrictions and sanctions must be consistent with the Mobile Phone Policy and boarding expectations. Boarders should know how to raise worries about online issues at any time, including out of hours.

12. Data protection, privacy and cyber security

Online safety monitoring must be carried out lawfully, proportionately and in accordance with data protection requirements. Monitoring data will be stored securely and accessed only by appropriate staff for safeguarding, behaviour, technical or legal purposes. The College will maintain appropriate cyber security controls, including password expectations, account management, access controls, software updates and incident response procedures.

Pupils and staff must not share passwords or login details. Suspected account compromise, phishing, malware, unauthorised access, data breach or cyber incident should be reported to IT Services and, where safeguarding may be involved, to the DSL. Suspected password or account breaches, whether deliberate, accidental or arising from external scams, must be reported to IT Services immediately and credentials changed or secured as directed.

12.1 Online use of pupil images

The College recognises the risk that pupil images may be copied, manipulated or misused online, including through AI image manipulation and the inappropriate use of smart spectacles/glasses or other devices with inbuilt cameras. Accordingly:

- the College aims to avoid using images which provide unnecessary identifiable information such as names;
- the College aims to avoid using images which are particularly easy to misuse or abuse;
- staff training will include image-security awareness and appropriate reporting of concerns about image capture, manipulation or misuse.

12.2 Recording, transcription and AI note-taking

Staff, pupils, parents/carers and visitors must not make an audio or video recording, use live transcription, automated note-taking or AI transcription software, or otherwise create a transcript or record of any lesson, meeting, parent forum, telephone/video call, conversation or other College interaction without the explicit prior permission of all parties whose contributions may be captured.

Where recording or transcription is agreed, it must be used only for the stated purpose and handled securely, with appropriate arrangements for access, sharing, storage and deletion. An exception may be formally authorised by the College for a legitimate safeguarding, accessibility, educational or legal reason, including a reasonable adjustment; any such arrangement must be agreed in advance and managed in accordance with safeguarding and data protection requirements.

13. Parents and carers

The College will work with parents and carers to support safe and healthy use of technology. Parent communication may include guidance on mobile-phone-free expectations, sleep and wellbeing, age-appropriate apps, parental controls, AI and deepfakes, online sexual imagery, sextortion, gaming, gambling, social media, reporting routes and sources of external support. This includes making clear that parents/carers must not record or transcribe College meetings, forums, calls or conversations without the explicit prior permission required by section 12.2.

Where an online safety issue affects a pupil's welfare, the College will usually involve parents unless doing so would increase risk to the pupil or compromise a safeguarding response.

14. Monitoring, review and records

The DSL will maintain oversight of serious online safety incidents and will review records periodically to identify themes, gaps and trends. Relevant trends will inform training, curriculum, parent communication, technical controls, behaviour systems and safeguarding practice.

This policy will be reviewed annually and sooner if there are significant statutory changes, serious incidents, new technologies, system changes or emerging pupil risks. The policy owner is the DSL, working with the Deputy Head (Pastoral), Director of IT Services, Online Safety Co-ordinator and relevant senior leaders. The review will also take account of the College's Prevent Duty risk assessment and, where relevant, the DfE's 'Plan technology for your school' guidance.

15. Useful links and sources of advice

- Keeping Children Safe in Education 2026 - DfE
- Mobile Phones in Schools: statutory guidance - DfE
- Filtering and Monitoring Standards - DfE
- Meeting Digital and Technology Standards in Schools and Colleges - DfE
- 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: advice for headteachers and school staff - DfE
- Internet Watch Foundation, CEOP, Childnet, NSPCC, Internet Matters, UK Safer Internet Centre and Professional Online Safety Helpline
- UK Online Harms Early Warning Working Group - guidance on protecting settings' images from AI manipulation and abuse: <https://d1xsi6mgo67kia.cloudfront.net/uploads/2026/05/Education-guidance-Protecting-your-settings-images-from-AI-manipulation-and-abuse.pdf>
- Safeguarding concerns: childprotection@bradfieldcollege.org.uk
- Professional Online Safety Helpline: 0844 381 4772

Last reviewed: August 2026. Next review: September 2027 Version 3.2

SRD