

Online Safety Policy

Berkhamsted Prep and Pre-Prep

Berkhamsted Senior Schools & Sixth

Heatherton

Charlotte House

Berkhamsted Day Nursery Ltd.

Berkhamsted School Enterprises Ltd.

Revision and Terminology: Please refer to the School's Policies Policy.

Policy owner:	Vice Principal
Type of policy:	Regulatory
Regulatory Body:	Department for Education; Independent Schools Inspectorate
Relevant Legislation / Guidance:	Education (Independent School Standards) Regulations 2014 as amended Keeping Children Safe in Education (2026)
Last reviewed by / date:	Exec on 10 September 2026
Last approved by / date:	Governors' Education Committee on 23 September 2026 Full Governors on 23 September 2026
Next review due:	Michaelmas 2029
This version published:	24 September 2026
Circulation:	☒ All Staff & Governors ☐ School Website ☒ Senior & Sixth Pupils ☒ Inspection Portal ☒ Parent Portal
Linked Policies:	Behaviour and Discipline Child Protection and Safeguarding (which includes the Staff Code of Conduct) Cyber Security IT Acceptable Use and AI (Pupils) IT Acceptable Use and AI (Staff) Prevention of Bullying Relationships Education and PSHE (Preps) RSE and PSHE (Senior & Sixth) Social Media Staff Protection

Contents

Scope of this policy	3
1 Core principles and delineation of responsibility	3
2 Scope.....	4
3 Review, evaluation and good practice	5
Appendix 1: Online Safety Guidance for Staff	7
1 Working online	7
2 Email, messaging and communications	7
3 Artificial Intelligence (AI)	8
4 Social media	9
5 Devices	11
6 Digital content.....	12
Appendix 2: Online Safety Provision for Pupils.....	13
1 Online hazards and managing risks	13
2 Security, identity and reputation	13
3 Online relationships.....	13
4 Digital citizenship and literacy.....	13
Appendix 3 – Online Safety and Awareness in the RSHE Curriculum	14
Appendix 4 - Filtering and Monitoring.....	16
Appendix 5 - Charlotte House School	17

Scope of this policy

I Core principles and delineation of responsibility

- 1.1 Educational technology helps pupils learn creatively and effectively. The School adopts an intentional blended learning approach, where staff select digital and non-digital methods according to the learning purpose. It encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Safety Policy encourages appropriate and safe behaviour during this process.
- 1.2 The promotion of positive behaviour at school will hopefully transfer directly into each pupil's adult life and prepare them for experiences and expectations in Higher Education or training and the workplace. This policy is not designed to be a blacklist of prohibited activities; it is a list of areas to discuss, teach and inform and will help the development of positive behaviour and knowledge, leading to safer internet use. The positive effects of the policy are intended to be seen online and offline in school and at home, and ultimately beyond school and into the workplace.
- 1.3 Online safety is regarded by Berkhamsted Schools Group as a facet of safeguarding and child protection. The approach taken by the school is that pupils, staff and parents who are equipped with a mature understanding of key safeguarding principles will be able to apply them equally to online safety.
- 1.4 Online safety therefore requires special treatment only insofar as signposting the use and application of general safeguarding principles to pupils, staff and parents.
- 1.5 The promotion of online safety is therefore the responsibility of all members of staff. Responsibility for the signposting of specific matters relating to online safety is shared by the school's team of Designated Senior Persons under the leadership of the Designated Safeguarding Leads. The Group Director of EdTech and the Head of Digital Learning in the Prep Schools are responsible for advising the DSLs and DSPs on online safety best practice and for developing resources that promote safe and responsible use of technology across the Foundation. They also provide strategic oversight of the effectiveness of the School's filtering and monitoring systems, ensuring that these are fit for purpose, operate effectively, and are regularly reviewed and evaluated to ensure they continue to meet safeguarding requirements and respond to emerging risks.
- 1.6 The School recognises both the educational value and the safeguarding risks of generative artificial intelligence. Staff and pupils must use AI only in accordance with the IT Acceptable Use and AI Policy, approved-tool and age requirements, data-protection expectations and task-specific guidance. Personal or sensitive data must not be entered into unapproved tools. Users should critically evaluate outputs for accuracy, bias, manipulation and inappropriate content, and should acknowledge AI use where required.
- 1.7 Opportunities and resources for teaching online safety are available at Annex A of KCSIE 2026.
- 1.8 **For the avoidance of doubt, anyone who has concerns regarding online safety should treat the matter as they would with any other safeguarding issue, by following the procedures detailed in the Child Protection and Safeguarding Policy. This includes the procedure for reporting concerns.**
- 1.9 Any concern involving AI-generated or digitally altered content; including sexualised

images, deepfakes, impersonation, bullying, discriminatory content, misinformation, grooming, scams or coercion, must be treated as a safeguarding concern and reported through the School's established safeguarding procedures. AI-generated nudes or semi-nudes are treated in the same way as other nude or semi-nude imagery, whether consensually or non-consensually made or shared. Staff should preserve available evidence without viewing, copying or forwarding illegal imagery and seek immediate advice from the DSL. Please refer to the School's Child Protection Policy for further information and guidance.

2 Scope

- 2.1 The School Online Safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related internet and computer systems internally and/or externally.
- 2.2 The School will make reasonable use of relevant legislation and guidelines to effect positive behaviour regarding IT and internet use on and off the school site. This will include imposing rewards and sanctions for behaviour and penalties for inappropriate behaviour as defined as 'regulation of student behaviour' under the Education and Inspections Act 2006. 'In loco parentis' provision under the Children Act 1989 allows the school to report and act on instances of cyber-bullying, abuse, harassment, malicious communication and grossly offensive material. This includes reporting to the police, social media websites, and hosting providers on behalf of pupils.
- 2.3 In line with KCSIE 2026, the School is mobile-phone-free during the school day by default. Pupils must not have access to mobile phones during lessons, movement time, breaks or lunchtime, except where an authorised, individual exception applies (e.g. medical). The School's phase specific arrangements, including Yondr procedures and the staged smartphone free approach, are set out in the Behaviour and Discipline Policy, IT Acceptable Use Policy and the Mobile Phone and Smart Device Policy.
- 2.4 The Online Safety policy covers the use of the following:
 - 2.4.1 School-based IT systems and equipment
 - 2.4.2 School-based intranet and networking
 - 2.4.3 School issued devices such as Surface Laptops/Pros
 - 2.4.4 Mobile devices (including phones) when used on the school site (both school owned and personal)
 - 2.4.5 Pupils' and staff's personal IT equipment when used in school and which makes use of school networking, file-serving and/or internet facilities
 - 2.4.6 External access to internal school networking including, but not limited to, Microsoft 365, Teams and printing
 - 2.4.7 School-related external internet including, but not limited to, extranet, online learning applications and platforms, blogs and social media platforms
 - 2.4.8 Use of personal devices in cases where offensive or inappropriate content or

contact can be connected to the School. Please see IT Acceptable Use and AI Policy for further details.

3 Review, evaluation and good practice

- 3.1 The school will keep up to date with best practice in online safety by:
 - 3.1.1
 - 3.1.2 I.I Having online safety as a standing item in the termly Safeguarding **meetings** attended by all DSPs, the DSLs and the Vice-Chair of Governors (the School's nominated Safeguarding Governor – see Child Protection and Safeguarding Policy).
- 3.2 The DSPs and DSLs will monitor and evaluate the Online Safety Policy. In the event of an online safety incident, the following people may be informed within school:
 - 3.2.1 Director of IT
 - 3.2.2 Group Director of EdTech
 - 3.2.3 Head of Digital Learning (Preps)
 - 3.2.4 Chief People Officer
 - 3.2.5 Heads of Department (if appropriate)
 - 3.2.6 Heads of House or Assistant Heads (if appropriate)
 - 3.2.7 Chief Operating Officer
 - 3.2.8 Data Protection Adviser
- 3.3 The Online Safety Policy will be reviewed as per the regular cycle of policy review (see Policies Policy). Additionally, the policy will be reviewed promptly upon:
 - 3.3.1 Advice from the police
 - 3.3.2 Online safety incidents in the community or local schools which might impact on the school community
 - 3.3.3 Significant changes in technology as used by the school or pupils in the wider community
 - 3.3.4 New guidance by Government/Local Authority/safeguarding authorities
 - 3.3.5 Serious and/or frequent breaches of the acceptable internet use policy or other in the light of online safety incidents
- 3.4 The School will factor online safety training, teaching and learning provision and parental events into the School calendar. This provision will be mapped and planned by the Group Director of EdTech in the Senior School and Group-wide, and by the Head of Digital Learning at the Prep, Pre-Prep and Heatherton. It will be delivered by those deemed most appropriate (as decided by the DSPs/DSLs).
- 3.5 The School also has a responsibility, as per Keeping Children Safe in Education, to:

- 3.5.1 Identify and assign roles and responsibilities to manage filtering and monitoring systems
 - 3.5.2 Review filtering and monitoring provision at least annually, with records of these reviews being retained.
 - 3.5.3 Block harmful and inappropriate content without unreasonably impacting teaching and learning
 - 3.5.4 Ensure effective monitoring strategies are in place that meet safeguarding needs
- 3.6 The effectiveness of provision will be reviewed at least once every academic year by Group Director of EdTech (Senior School & Group-wide) supported by the DSL and IT. Records of checks, findings, decisions and actions will be retained in the Safeguarding Team by Group Director of EdTech (Senior School & Group-wide).

Appendix I: Online Safety Guidance for Staff

I Working online

- 1.1 Online safety education is included in the curriculum, in order to foster age-appropriate autonomy, digital resilience and ethical digital participation. The School considers our approach to be both pro-technology and pro-boundaries. Online safety is the space where safeguarding, technology, community, education and wellbeing all converge. This approach supports intentional blended learning: digital access is purposeful, age-appropriate and balanced with device-free teaching and learning. Staff understand the safeguarding risks associated with AI technologies and follow the IT Acceptable Use and AI Policy.
- 1.2 Staff should always carefully plan teaching and learning activities involving digital resources, ensuring that they have thoroughly tested them for suitability and functionality. Any online resources or tools for use in class should be assessed by the teacher prior to the lesson to ensure that they are age-appropriate and safe for use. If testing new digital tools, staff should seek advice from the Group Ed Tech Director (Senior Schools, Sixth and Group-wide) / Head of Digital Learning (Preps), Director of IT and IT Support.
- 1.3 Whenever working with pupils online, staff should reinforce key messages about behaving in a safe and responsible manner, being critically aware of the content they access and acknowledging their sources of information. All staff should model good and safe practice in their own use of digital tools and services.
- 1.4 Where pupils work online, staff must maintain active supervision and, where appropriate, use Lightspeed Classroom or the School's current classroom-management platform. Lightspeed Filter and Alert form part of the School's wider safeguarding filtering and monitoring arrangements. When using personal devices, pupils remain subject to the School's expectations for online conduct. Staff are trained to understand the filtering and monitoring systems that operate in School and processes that are in place if a pupil uses their device or the School network inappropriately.
- 1.5 Staff should take seriously any pupil disclosure regarding online bullying or misconduct and report it appropriately. **Please see the Child Protection & Safeguarding Policy, and the Prevention of Bullying Policy for further details.**
- 1.6 Where filtering restricts a resource required for teaching, staff may submit a request to the Group Director of EdTech (Senior School & Group-wide) and IT Support. The request will be assessed taking account of curriculum need, safeguarding, data compliance, accessibility and available alternatives.
- 1.7 Sometimes the internet filtering system blocks sites that teachers wish to use for lessons. In this case, a request to IT Support can be made to remove the site from the filtered list.

2 Email, messaging and communications

- 2.1 Staff should only use official School email accounts and telephone numbers for School-

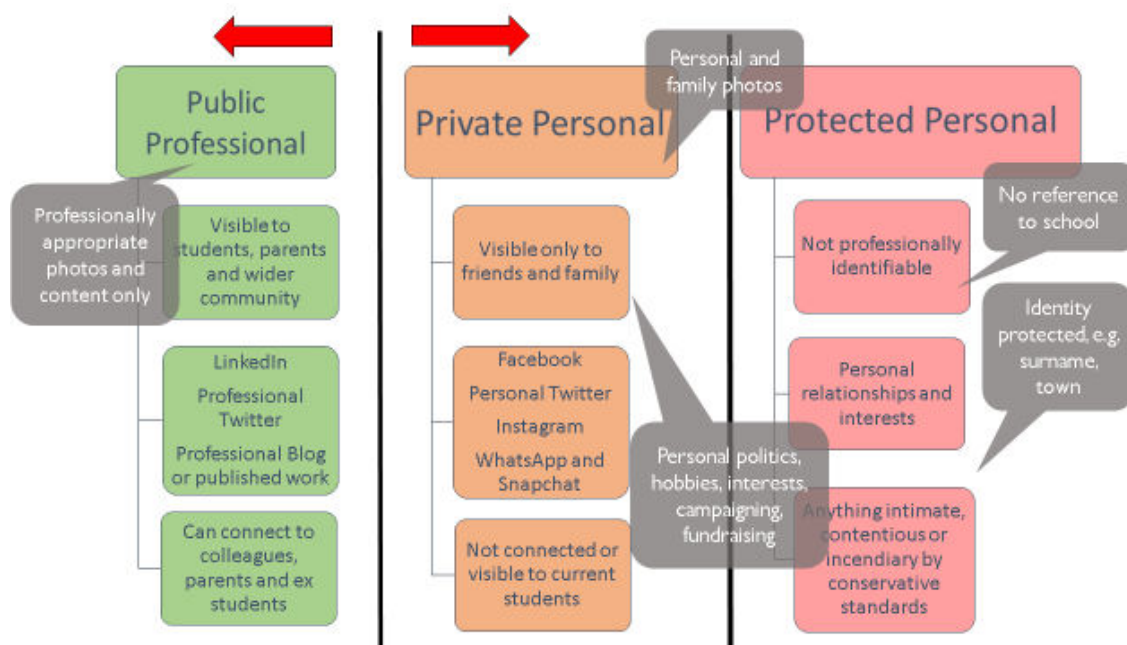
- related matters, contact with other professionals for work purposes, and to communicate with pupils, parents or carers. Personal email accounts and telephone numbers should not be used for School-related communications, either directly, or via third-party applications.
- 2.2 School email addresses and telephone numbers should not be associated with online accounts or services that are for personal use, including social media, online communications and messaging applications.
 - 2.3 Messages sent from School accounts should be professionally and carefully written. Staff are representing the School at all times and should bear this in mind when entering into any online communications.
 - 2.4 For any challenging or sensitive issues or anything that may have legal repercussions, staff should have the content of their message checked carefully by their line manager or a member of the Senior Management Team.
 - 2.5 Staff must tell their line manager or a member of Senior Management Team if they receive any offensive, threatening or unsuitable messages, from either within the School or from an external account. They should not attempt to deal with these themselves. Please see the Staff Protection Policy for further details.
 - 2.6 Staff should be mindful that whilst email and messaging is very important for the effective functioning of the school, it adds to workload. Staff should ensure that their communications are clear, concise and sent only to the individuals or groups required. Particular care should be taken with using the "Reply All" function, and the appropriate use of group mailing lists.
 - 2.7 Staff should adhere to the School's email curfew and avoid sending email between the hours of 7pm and 7am; instead using the delayed delivery function on Outlook outside of those times.
 - 2.8 The forwarding of chain messages is not permitted in School.
 - 2.9 Staff have responsibility to ensure that they treat suspect email (spam) with suspicion and deal with it appropriately. All staff are required to engage with the School's cybersecurity awareness programme, including Pistachio training and phishing simulations, to help identify and respond appropriately to phishing and other cyber threats.
 - 2.10 Staff should endeavour to use the most appropriate channel for communication (email, Microsoft Teams chat, a shared document, etc.) according to the message and the audience.

3 Artificial Intelligence (AI)

- 3.1 The School recognises the growing use of artificial intelligence (AI) technologies. Staff and students should use only approved AI tools and must not disclose personal, confidential or sensitive information to AI systems without appropriate authorisation. Users should remain critical of AI-generated content, recognising that it may be inaccurate, misleading or biased, and should verify information before relying upon it for educational or business purposes. **Please see the IT Acceptable Use and AI Policy for further details.**

4 Social media

- 4.1 The School expects all staff and pupils to remember that they are representing the School and must act accordingly online as well as offline.
- 4.2 Staff should protect pupils by ensuring that school-provided platforms and services are the default online tools used for collaboration and communication. Using other online networks or social media for school-related purposes to communicate, collaborate or publish pupils' work should only be done in agreement with the Group Director of EdTech (Senior Schools and Sixth) / Head of Digital Learning (Preps) and the IT Strategy Group. It is not appropriate to deploy tools which provide unmonitored private channels of communication between users.
- 4.3 Staff who run **official School social media accounts** (an Instagram account, for example) should refer to the Social Media Policy for further information and guidance.
- 4.4 Individual staff may choose to run **public professional social media accounts** on their own behalf for the purposes of engaging in educational debate, sharing best practice, professional development and networking. Such accounts can be an asset to the individual and the school as a learning community. Public professional accounts should include an appropriate profile photograph, can refer to and engage with Berkhamsted School content in a professionally appropriate way, and should not include personal content.



- 4.5 Staff becoming 'friends' or connecting with pupils on social networks is not appropriate under any circumstances, and Staff should only use public professional accounts when connecting with parents or former pupils (see diagram above). Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the Staff Code of Conduct (in the Child Protection and Safeguarding Policy) and

IT Acceptable Use Policy (Staff).

- 4.6 Staff should proactively create and maintain an appropriate boundary between professional and personal uses of social media, taking care to ensure that privacy settings are used to their best effect. It is common in digital spaces to find that the lines between the professional and the personal can appear less distinct. However, teachers and those who work in educational settings are held to very high standards of behaviour indeed, so it is strongly advised that staff keep all **private personal** and **protected personal** accounts away from public view, and visible only to friends and family.
- 4.7 Content shared from official Berkhamsted School social media channels is monitored regularly for branding, engagement and reach purposes, and the School aims to uphold a high standard of quality and interaction. Staff with public professional accounts are encouraged to engage with the Berkhamsted content online by following, liking, sharing/retweeting and commenting. However, staff using personal accounts should first ensure that their privacy settings protect their timelines from prying eyes, since such interactions will make their personal account name publicly visible to anyone else engaging with the same content.

Regular brand monitoring will pick up search results on key words. Staff should expect that their social media account is picked up in such searches and treated as a *de facto* public professional account if it is:

a) **Publicly visible**

AND

- b) **Clearly associated with Berkhamsted Schools Group** either by (any two of the following)
- The user's full name being used in the ID or bio
 - The School is named in the bio, or an obvious connection to the School without scrolling very far
 - The creation, sharing or interaction with School-related content

The results of the searches of social media content are divided into three categories.

- Optimal:** Messaging is relevant to school life, helpful and appropriate for the targeted audience and in alignment with school values. Messages of this nature are encouraged to include the brand hashtag #teamberko. The official School accounts are encouraged to share or engage with these messages.
- Sub-optimal:** Messaging is only tenuously or partially linked to school life, is out of kilter with conservative audience expectations for that channel or account, or is at odds with school values.
- Critical:** Messaging compromises the School's reputation or personal reputation of one of

our school community. Messages of this nature are offensive, harmful, derogatory, extreme or inappropriate **either directly or indirectly** (i.e. by association). There are no positive links to school life, the content would be seen in a poor light by conservative audience and is counter to school values.

Sub-optimal content will be dealt with on a discretionary basis and may be reported to line managers. Critical content will be reported to the Principal (or Vice Principal in absence) and may be subject to disciplinary procedures.

- 4.8 If staff run multiple accounts from a single device, they should take extra care with following, sharing and engaging with content in order to avoid confusing personal and professional accounts.
- 4.9 When creating or engaging with content online, (even from a private personal account) it is important that staff consider the viewpoints and agendas of those who might scrutinise their online actions, including, but not limited to: curious past, prospective or existing parents, the current school community, future employers, journalists, past or present pupils, trolls, stalkers, catfishers, scammers, and would-be blackmailers.
- 4.10 Staff should be cautious about using social media companies to sign in to other services e.g. review websites, retail platforms and dating apps, and where social media accounts connect, e.g. If your Instagram account automatically posts to Twitter.
- 4.11 Staff should be aware that their reputation may be harmed by what others share about them publicly online, such as friends tagging them in inappropriate posts, photographs or videos. Discussing the issues around sharing and privacy settings with friends, family and colleagues may help in preventing issues arising, as well as ensuring that privacy settings are used effectively.

Please see the IT Acceptable Use and AI Policy for further details.

5 Devices

- 5.1 Staff must not use their own personal mobile phones to contact pupils or parents either in or out of School time (via personal email addresses, messaging services or third-party apps excluding the school's learning platform) unless in an emergency.
- 5.2 Staff choosing to use a personal device to connect to school services (for email for example) and professional mobile devices belonging to staff must be passcode protected, set to wipe after failed login attempts and connected to Find My (for Apple) and Find My Device (for Android) to protect school and personal data in case of loss or theft.
- 5.3 Staff should never leave a school device unattended when logged in. Devices should be locked or staff should log off.
- 5.4 Staff should only use School devices to take photos or record videos in a professional capacity. For KS2 and above, if this is not feasible, personal devices may only be used to take photographs with permission from the relevant Headteacher. For the avoidance of

doubt, personal devices must never be used for this purpose in EYFS and KS1.

- 5.5 Staff should take special care to log out of any online accounts when returning borrowed IT equipment, such as school iPads.
- 5.6 The loss, damage or theft of school devices should be reported as soon as possible.

6 Digital content

- 6.1 Staff are allowed to take photographs or record video in school to support educational aims but must follow different school procedures concerning the sharing, distribution and publication of those images. In order to prevent allegations of inappropriate activity, staff may not store images of pupils on personal devices or in personal cloud-based storage. Any images taken on personal devices (see 4.4, above) must be moved to School systems as soon as is reasonably possible and the personal copy permanently removed.
- 6.2 Photographs or video of pupils should only be published online publicly via official school channels. For example, it is inappropriate for staff to publish video of a school event to a personal YouTube account or Facebook page, or to post photographs of pupils to a private personal Social Media account.
- 6.3 Staff should refer to the Social Media Policy for guidance about publishing photographs or video of pupils on official School social media channels, including the appropriate use of names.
- 6.4 Staff must not store pupil data on memory sticks or external hard drives and should refer to the Data Protection Policy and the Information Security Policy for further information.

Appendix 2: Online Safety Provision for Pupils

Online safety education is planned progressively by age and stage and delivered through the curriculum, Personal Development (PSHE), pupil induction and whole School provision. It includes the four areas of online risk; content, contact, conduct and commerce, together with digital wellbeing, healthy relationships, critical literacy, privacy, security, reputation and the safe, responsible and ethical use of AI.

Teachers should be aware of the opportunities and resources available in Annex A of KCSIE 2026

The outline of key themes is as follows:

1 Online hazards and managing risks

- 1.1 Inappropriate and offensive material
- 1.2 Grooming and online predators
- 1.3 Bullying and trolling

2 Security, identity and reputation

- 2.1 Digital footprint
- 2.2 Passwords
- 2.3 Social media profiles and privacy settings
- 2.4 Identity theft

3 Online relationships

- 3.1 Sexting, image sharing and the law
- 3.2 Pornography, body image and healthy relationships
- 3.3 Making or sharing nudes and semi-nudes, including non-consensual, digitally altered or AI-generated images

4 Digital citizenship and literacy

- 4.1 Illegal downloads
- 4.2 Spam, scams, phishing and data harvesting
- 4.3 Copyright, plagiarism and referencing
- 4.4 Safe search
- 4.5 Understanding fake news, bias, misinformation and credibility
- 4.6 Safe, responsible and ethical use of artificial intelligence; AI-generated misinformation, deepfakes and impersonation; privacy, intellectual property and algorithmic bias; recognising AI-enabled scams and manipulation; and how to report harmful, abusive or sexualised synthetic content.

Appendix 3 – Online Safety and Awareness in the RSHE Curriculum

Relationships Education, Relationships and Sex Education (RSE) and Health Education statutory guidance (updated in July 2025)

Primary

1. That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.
2. How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.
3. That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
4. The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
5. Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
6. That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

Secondary

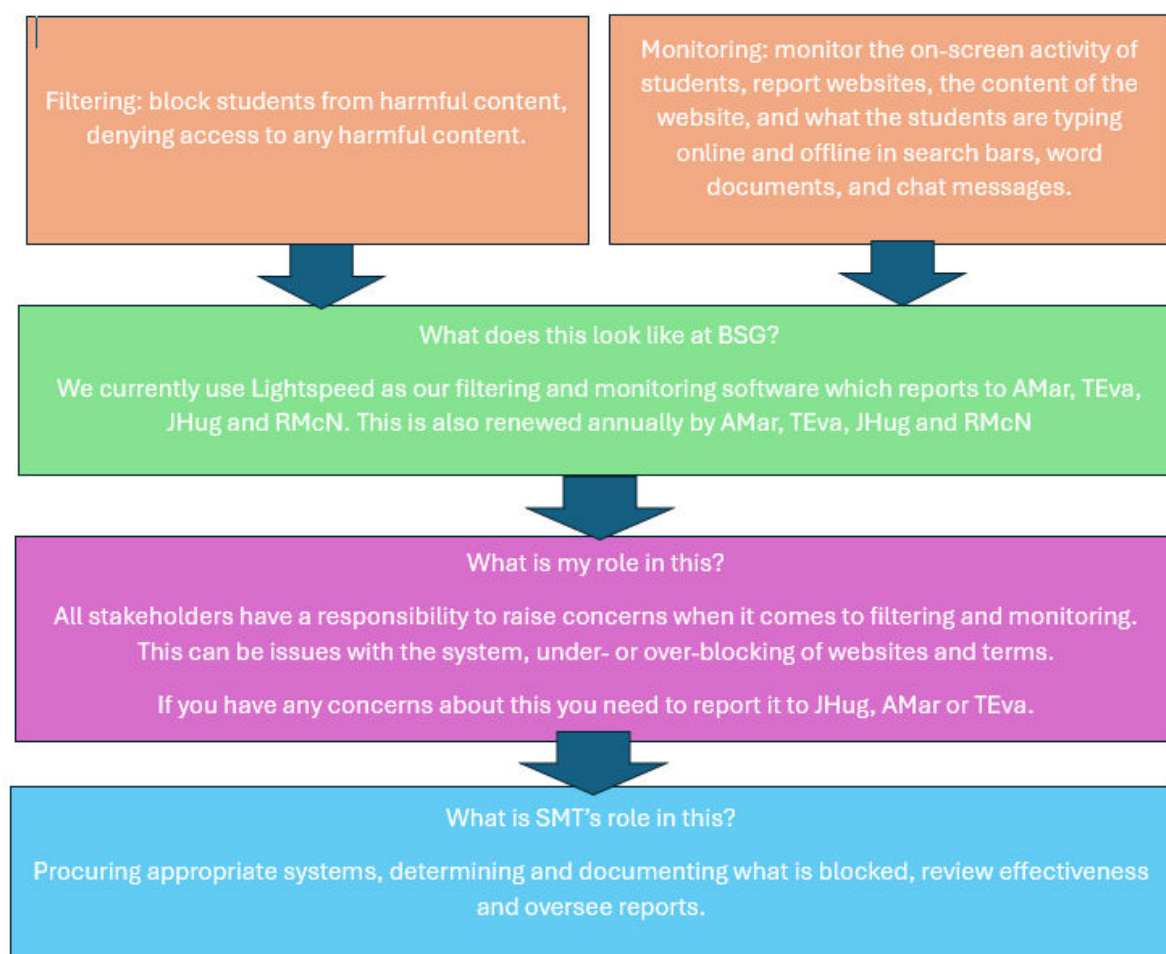
1. Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
2. Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues.
3. The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online.
4. Not to provide material to others that they would not want to be distributed further and

not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images.

5. That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime.
6. What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online.
7. About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them.
8. That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong.
9. That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice.
10. How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns.
11. That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it.
12. How information and data is generated, collected, shared and used online.
13. That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising).
14. That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.
15. That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk.

Appendix 4 - Filtering and Monitoring

Berkhamsted Schools Group: **Filtering and Monitoring Overview**



Appendix 5 - Charlotte House School

This appendix outlines the specific operational variances and software platforms. Over time Charlotte House will adopt the BSG software and processes.

I. Key Operational & System Variations

Operational Area	Berkhamsted Schools Group Standard	Charlotte House Local Variation / System
Pupil Virtual Learning Environment (VLE) & Email	Microsoft 365 / Teams	Google Classroom / Google Drive: Prep pupils are issued personal Google Classroom addresses for remote learning and assignment submission.
Incident Reporting Software (Pupil Screen)	Group Monitoring / Reporting tools (e.g., Senso)	BEESAFE Icon: Pupils use the "BEESAFE" icon on their screen to immediately flag inappropriate or disturbing material.
Search Engines for Remote / Home Learning	Standard Group-filtered access	Kiddle: Recommended child-safe search engine (\$https://www.kiddle.co/\$) for independent home research tasks.
External IT Support / Technical Escalations	Internal Group IT Support & Group Ed Tech Director	Beebug / External IT Consultant: Local technical support and filtering escalation contact alongside the internal Bursar.