



Online Safety and Acceptable Use Policy 2026-2027

This policy aims to proactively promote a safe and secure digital environment and encourage positive behaviours for all members of the community at Knightsbridge School, a member of the Dukes Education Group. It is designed to ensure compliance with relevant UK legislation, and has been prepared with reference to the statutory guidance from the Department for Education's Keeping children safe in education, September 2026 (KCSiE 2026).

Specifically, this policy will help:

- Safeguard pupils and staff when using devices and online technologies, both on and off the school premises
- Promote the safe and responsible use of devices and online technologies
- Provide clear guidelines on appropriate online behaviour for pupils and staff including any sanctions that may result in the event there are infringements
- Raise awareness of both persistent and trending digital and online safety risks
- Provide mechanisms for easily reporting and addressing online safety concerns
- Prevent data breaches & cyber incidents

This policy should be understood in the context of other relevant school policies and procedures, especially the *Safeguarding and Child Protection Policy*, the *Behaviour and Discipline Policy*, the *Anti-Bullying Policy*, the *Staff Code of Conduct Policy*, the *Child on Child Abuse Policy*, the *Distance Teaching and Learning Policy*, the *Staff Acceptable Use Agreement* and the *Pupil Acceptable Use Agreements*. By accessing and using the school network, all users automatically agree to abide by the expectations set out in the *Acceptable Use Agreements* and this policy. Online Safety and Acceptable Use at Knightsbridge School reflects provisions in the school's Safeguarding Child Protection Policy related to online behaviours and includes commitments for the appropriate filtering and monitoring on school managed devices and systems. It also acknowledges that some children may have access to personal smartphones and mobile networks and how this is managed at Knightsbridge School.

Scope

This policy applies to all members of the school community including staff, pupils, volunteers, parents/guardians, directors/governors and visitors. That is, anyone who uses the school IT systems, services or devices; on or off the school premises; including anyone accessing the school's IT systems or services from non-school owned devices. All individuals within this scope are expected to read, understand, and comply with this policy.

To keep our students safe, the law gives us the authority to address student misbehaviour, even when it happens outside of school hours or off school grounds. This includes issues like cyber-bullying or other online safety concerns that affect our school community.

Under the Education Acts of 2006 and 2011, if we have good reason, we can search a student's electronic device and delete any harmful or inappropriate content. We will only take action on issues that fall under our school's policies for Safeguarding, Child-on-Child Abuse, and Behaviour. Whenever possible, we will inform parents about any incidents of inappropriate online behaviour that happen outside of school.

We also have a legal duty to prevent students from being drawn into terrorism, and our policies reflect the latest government guidance on this.

Further, we should all be aware that technology is a significant component in many safeguarding and wellbeing cases. Children are at risk of abuse online as well as in person. In many cases abuse will take place concurrently both online and offline. Children can also abuse other children online, it can be consensual or non-consensual and can take many forms including harassing, misogynistic or misandrist messages, coercion, and the sharing of abusive images or pornography.

Categories of Online Risks

KCSIE 2026 outlines four high-level areas of online safety risk:

- **Content:** Being exposed to illegal, inappropriate, or harmful content - including misinformation, disinformation (fake news), conspiracy theories, extreme violence, misogyny, and harmful AI-generated media.
- **Contact:** Being subjected to harmful online interaction with other users or non-human entities (e.g., generative AI models and chatbots).
- **Conduct:** Personal online behaviour(s) that increase the likelihood of harm, such as cyberbullying, harassment, trolling, or creating, sending, and sharing explicit images (including AI-generated images).
- **Commerce:** Risks such as online gambling, financial scams, phishing, unauthorised in-game purchases, target advertising, and inappropriate personal data sharing.

Most safeguarding risks present in the physical world can extend into the digital world and become amplified online. In response:

- **Content:** The school employs appropriate filtering and monitoring systems that alert relevant staff to behaviours that may be putting children at risk. These systems are regularly updated with threat intelligence to prevent access to illegal, inappropriate, or harmful content, including AI-generated harms.
- **Contact and interaction:** Measures are in place to monitor and minimise harmful interactions online, including child-on-child risks (cyberbullying, sharing explicit/AI-generated images, peer pressure), interactions with AI chatbots, and adult-posed risks such as online grooming, exploitation, and radicalisation.
- **Conduct and online behaviour:** The school teaches pupils and staff about responsible online behaviour, highlighting the risks of sharing explicit or AI-manipulated images, engaging in online trolling, harassment, or bullying.
- **Commercial risks:** Online safety learning includes age-appropriate content covering risks such as the inappropriate sharing of personal data or images, engaging with in-game purchases, financial/online scams, online gambling, and infringing intellectual property.

Current Risk Landscape

The following risks are considered current and most pertinent to pupils, staff and our wider school community:

- Online hate, misogyny, violence, conspiracy, fake news and the spreading of false information
- Cyberbullying, especially on personal messaging apps and in-game chat
- Health and well-being as a result of the amount of time spent online/gaming
- Inappropriate disclosure (and use) of personal information
- Sending, receiving or using of personal images or data (including that of a sexual nature)
- Lack of care or consideration for the personal data and/or intellectual property of others
- Not verifying the authenticity or accuracy of online content
- Ignorance of one's digital footprint and online reputation
- Online grooming
- Hacking of accounts or impersonating another person, devices and data including identity theft via email phishing campaigns or through compromised or spoof websites and online services including using someone else's digital identity
- Risk of radicalisation and/or access to online content that may lead to indoctrination into any form of extreme ideology
- Risk of AI generated video, audio, images or text that is intended to deceive, defraud, harm or elicit a reactive response
- Using personal devices/mobile networks while at school and/or unapproved online tools, services & subscriptions in the context of school
- Misuse of personal information and data, including unauthorised data collection by third-party apps and services
- Generating, requesting, or distributing sexually explicit, defamatory, or abusive content depicting members of the school community
- Involuntary celibate (incel) ideologies, extreme influencer harm, and automated algorithmic risks on video-sharing platforms

Roles and responsibilities

Governors/Directors

Knightsbridge School relies on the wider Dukes Education Group to ensure that all Governors/Directors:

- Have a strategic responsibility for their school's safeguarding arrangements, including online, and must ensure that the school and its staff comply with their duties under legislation
- Receive appropriate safeguarding & child protection training, including online at induction and are regularly updated, at least annually
- Are fully informed of the school's duty with regard to current UK data protection legislation especially in regard to the processing of personal information fairly and lawfully and to keep the information they hold safe and secure
- Support the SLT in fulfilling their digital and online safety responsibilities, especially those relating to safeguarding children and anywhere the school has a legal responsibility to uphold.

Senior Leadership Team (SLT)

- This policy is implemented and reviewed at least every year

- Procedures are in place so all staff understand and can carry out their IT and online safety responsibilities especially those relating to the safeguarding of children
- All staff undergo regular safeguarding training including online safety, which amongst other things includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- All staff are provided with Data Protection training at induction/at least annually in line with the schools responsibilities under current UK data protection legislation, especially to process personal information fairly and lawfully and to keep the information they hold safe and secure
- The school has appropriate filtering and monitoring systems in place and the staff responsible for managing them do all that is reasonable to limit children's exposure to the risks posed when using the schools IT systems and working online
- Online safety is a running and interrelated theme and part of the whole school approach to safeguarding
- They maintain executive oversight of the regular review of i) this policy; ii) the staff ICT and online safety training; iii) online filtering and monitoring provisions; and to ensure the relevant staff and external providers meet our own high standards and legal commitments
- Annual risk assessments are conducted, including those related to AI
- Ensure all staff understand and carry out their ICT and online safety responsibilities especially those relating to the safeguarding of children
- Are fully informed of the school's duty in regard of current UK data protection legislation especially to process personal information fairly and lawfully and to keep the information they hold safe and secure
- Provide support and assistance to the DSL, the deputy DSL and the eSafety Officer, while reporting to the Head on all matters relating to digital and online safety
- Ensure that children across all school sections are taught with up to date, age appropriate content and language, about how to keep themselves and others safe when using digital technology and when online
- Promote and raise awareness of digital and online safety issues with parents and the wider school community at every opportunity
- Have oversight and ensure appropriate sanctions are actioned in behaviour instances relating to online safety, acceptable use, and cyberbullying

Designated Safeguarding Lead (DSL) and Deputies

- Takes lead responsibility for safeguarding and child protection including having oversight of the all online safety procedures
- Take the lead role in responding to filtering and monitoring alerts, regularly reporting trends to SLT and Safeguarding Governor; and liaise with the eSafety Officer & the IT team to ensure the systems are working effectively
- Liaise and support the school's eSafety Officer, SLT, IT team, and all relevant staff in matters relating to safeguarding children in physical, digital and online environments while reporting to the Head and Safeguarding Governor on these matters
- Understand the risks to children associated with digital and online technologies and are confident that they have the capacity to keep children safe from harm
- Have oversight of digital and online safety documentation, procedures and training to ensure that they are aligned with the schools safeguarding responsibilities

eSafety Officer

- Takes a leading role for digital and online safety issues across the school

- With support from the IT team, has the primary role in preparing, updating and reviewing this policy; the *Staff and Pupil Acceptable Use Agreements* and the *Home-School Contract for the Safe use of The Internet and Digital Technologies* and the schools *Policy for Distance Teaching and Learning*
- Takes a lead role in the regular review of the prevailing digital and online risks landscape, and a supporting role in the regular review of the provision for filtering and monitoring
- With the support from Heads of Sections (EYFS, Junior & Senior), ensures that all pupils are aware of the expectations documented in the applicable age appropriate *Acceptable Use Agreements* and the *Home-School Contract for the Safe use of The Internet and Digital Technologies*
- Is responsible for organising and delivering digital and online safety training as well as providing advice to staff, children and parents on these matters
- Collaborates with the DSL, IT Team, and relevant academic staff to conduct the annual online safety review and risk assessment
- With the support of HR ensures all staff have reviewed this policy and the Staff Acceptable Use Agreement
- Takes a leading role, liaises and advises the Designated Safeguarding Lead (and deputies), in all matters concerning digital and online safety
- With the support from Heads of Sections (EYFS, Junior & Senior), ensures that all children are taught how to keep themselves and others safe when using technology and when online
- Demonstrates leadership in the schools commitment to keep current the digital and online safety learning content, and that it is a running and interrelated theme across the curriculum and part of the whole school approach to safeguarding
- Liaises with the school IT team to ensure that filtering and monitoring is working effectively without overblocking, and collaborates on all other relevant digital, online safety and cyber security matters
- Supports the DSL & their deputies in the day to day response to filtering and monitoring alerts; understands trends and reports whenever necessary to SLT
- Acts as a primary liaison for all digital and online safety concerns raised by pupils, staff and any other member of the school community
- Communicates regularly with SLT and the DSL and deputies to discuss current issues and trends
- Keeps current with digital and online trends, the safety issues associated with them and updates to relevant legislation, especially that which relates to the safeguarding of children

IT Team

- Responsible for the provisioning, operation & maintenance of filtering, monitoring and alerting systems including alignment with vendor best practices
- Takes a lead role in the periodic review of the technical provision for filtering and monitoring and a supporting role in the regular review of the current digital and online safety risk landscape
- Play a supporting role in responding to filtering & monitoring alerts and provide assistance to the DSL and deputies, the eSafety Officer and SLT when investigating digital and online safety incidents, including event logs analysis and digital evidence gathering
- Provide strategic advice on appropriate technologies to ensure the school upholds its digital and online safety obligations
- Keep current with technologies and industry trends related to digital and online safety, cyber-security and data security

- Supports the DSL (and deputies) and the eSafety Officer in the preparation, update and review of this policy; the staff and pupil *Acceptable Use Agreements* and the schools *Policy for Distance Teaching and Learning*
- Ensure the school network and systems are appropriately monitored in order that any misuse or attempted misuse can be identified and investigated
- Maintain frequent backups of critical data (at least daily) and systems (at least weekly); ensures encrypted copies of these backups are stored securely in more than one location, are locked to prevent accidental or malicious corruption and recovery routines are tested routinely in order that critical data and systems can be recovered in a timely fashion when required. This includes a clear, documented disaster recovery plan
- Supports the school's compliance with the DfE's Filtering and Monitoring Standards, ensuring the technical provision is appropriate for the school's context and safeguarding needs
- Makes sure all staff access to school IT systems is secured with unique credentials and protection is further enhanced with multi-factor authentication (MFA) wherever possible, but obligatory for staff access to email and privileged systems administrator access
- Deploy, maintain and monitor an appropriate end-point detection and response (EDR) system on all necessary school managed devices
- Patch and maintain systems and software ensuring all patches rated as "critical" are installed with 7-14 days of release
- Configure and maintain a strong email security stance to protect against phishing and email borne threats
- Manage, maintain and monitor a secure gateway(s) between the school private network(s) and the internet
- Oversee regular staff cybersecurity training including phishing simulations
- Manage systems hardware and software life cycles so that unsupported and in-secure systems are decommissioned in a timely manner; failing this, put in place mitigations in order to manage the risk(s) they pose until they can be fully decommissioned
- Maintain up-to-date documentation of the school's systems and services including maintaining and audit of all software and hardware assets on the school network(s)
- Provide support to, and liaise with, the DSL and deputies and the eSafety Officer on digital and online safety issues, and on IT and data security matters

Teachers

- Demonstrate good digital and online safety behaviours throughout all areas of practice
- Liaise with the eSafety Officer to incorporate digital and online safety learning into their curriculum/lesson plans, and always take opportunities to include online safety learning points wherever appropriate
- Guide and supervise pupils with care when engaging in digital and online activities (including extra-curricular and extended school activities), and be alert to the risks and harms that may present
- Help pupils build critical research skills by cross referencing sources, disregarding fake news and false information and help develop awareness of the legal issues relating to digital content such as copyright laws and plagiarism
- Teach children to keep themselves safe, including online and when accessing remote learning
- Take responsibility for checking online content before using it in class and reporting all instances where inappropriate content gets through the web filter. This includes evaluating the safety and appropriateness of AI tools before integrating them into lessons in line with the school's AI Policy

All staff

- Must take responsibility to be familiar with this policy and understand and agree to the Staff Acceptable Use Agreement (documented in the Safeguarding Policy). If there is anything you do not understand you must seek help from the eSafety Officer or DSL
- Report any online safety concern to the eSafety Officer, and the DSL (or a deputy) without delay whenever there is a possibility of harm to a child or other person
- Recognise that some categories of children are potentially at greater risk of harm than others both online and offline, for example, those with special educational needs
- Set a positive example by demonstrating responsible digital and online behaviours
- Guide others in the safe use of technology
- Understand current UK data privacy legislation in the context of their work at school
- Attend and complete regular up to date safeguarding, online safety training, including all cyber-security and data privacy training

Pupils

- Be open to learn about and adopt good digital and online safety practices and show this in the way you use technology and when online, both in, and out of school
- Be kind and mindful of your own and others safety when using devices and when online
- Always tell your teacher or trusted member of school staff straight away if you know of, see or receive digital or online content that makes you feel unhappy, worried or vulnerable
- If a personal smartphone or internet connected device is brought to school it must be handed in at the very start of each school day and collected on dismissal
- Pupil Acceptable Use Agreements:
 - Reception and Junior pupils (Years 1-6) - school planners have a page explaining "how we stay safe when using computers"
 - For all pupils (Years 3-11) - students will complete an online Acceptable Use Agreement at the start of each academic year (or when you join the school)

All pupils: i) will be inducted in the safe use of digital and online technologies at the start of each year, and ii) parents and guardians should familiarise themselves and their child/children with this policy

Parents and Guardians

- Familiarise yourself with the schools *Online Safety and Acceptable Use Policy* on behalf of you and your child
- Be aware that online filtering and monitoring are enforced on school systems and online services as part of our commitment to safeguarding children and in line with our legal obligations under KCSiE 2026
- Each year we offer parent specific eSafety and online training, and we encourage you to attend
- Support the school's commitment to online safety by learning and reinforcing the same positive behaviours and principles when children are at home and in your care
- Be vigilant when your child is online and always be sure you know who, if anyone, they are interacting with
- Contact the eSafety Officer, DSL or other member of school staff if they ever have a concern about their children's online activities or use of digital technology
- Smart phones and all other mobile electronic devices must be on silent or switched off and should not be used whenever in the presence of pupils at the school. Any exceptions to this must be sought and granted by the Head

- Note that the school website, parent portal or any other IT system made available to you is done so in accordance with the specific Terms, Conditions and Privacy stipulations published by each service

Visitors & Contractors

- If access to schools IT systems to carry out duties on behalf of the school are required, visitors & contractors must first obtain approval from the eSafety Officer or member of the SLT and agree to the Staff Acceptable Use Agreement
- Smart phones and all other mobile electronic devices must be on silent or switched off and should not be used whenever in the presence of pupils at the school. Any exceptions to this must be sought and granted by the Head

Filtering & Monitoring

- The school has appropriate filtering and monitoring systems in place and reviews their effectiveness each year. This review is part of the annual risk assessment process and is led by the DSL, eSafety Officer, and IT Team
- The leadership team and relevant staff have an awareness and understanding of the provisions in place for filtering and monitoring and ensure that they are managed effectively
- The school is committed to striking a balance between protecting students and allowing appropriate access for teaching and learning, as per the DfE standards
- There is a process in place for escalating and dealing with concerns about filtering and monitoring systems themselves. In all cases, concerns should be first addressed to the DSL (or a deputy), whether there is, or is not, an immediate concern for the wellbeing of a child or other person. The DSL or a deputy will involve the eSafety Officer and the IT team in order to address the concerns raised
- The school has taken into consideration the number of and age range of children (including those who are potentially at greater risk of harm) and how often they access school digital and online systems and have implemented filtering and monitoring solution(s) that on balance, mitigate against the safeguarding risks. We will reassess this provision on an annual basis

Further, in line with the [DfE - Filtering & Monitoring Standards](#), this school:

- Has assigned roles and responsibilities to manage filtering and monitoring as listed in the preceding paragraphs. In addition, the DSL (and deputies), the eSafety Officer and the IT Team will investigate all concerns raised about the schools filtering and monitoring systems
- Always aims to block harmful and inappropriate content without unreasonably impacting teaching and learning
- Embed monitoring strategies to help meet our safeguarding responsibilities. These include i) physical monitoring by teachers and teaching assistants watching the screens of pupils; ii) monitoring of network network traffic and online activities; and iv) the filtering and monitoring of activity on school managed devices

Remote Education

School communications with parents and guardians are used to reinforce the importance of keeping children safe online and we understand that parents and carers are likely to find it helpful to understand how the school filters and monitors online use. We shall always take the opportunity to make parents and guardians aware of what their children are being asked to do online, including i) the sites they will be asked to access, and ii) who from the school (if anyone) their child is going

to be interacting with online. For further information please refer to the school *Policy for Distance Teaching and Learning*.

Use of Personal Mobile Devices

This school does not allow the use of personal mobile or non-school managed devices by children while in school. However despite this, we acknowledge the risk that some pupils, on occasion, may have access to personal mobile networks and unfiltered internet access while at school and that this un-filtered and un-monitored activity can lead to inappropriate materials and behaviours on the school premises. In addition, to uphold our responsibilities as an EYFS setting, and to promote positive behaviour, we expect staff to limit their use of personal devices to areas that are not shared with, or in sight of, children (for example, the staffroom and other closed office spaces), unless prior written agreement is granted by the a member of the SLT in consultation with the DSL. In addition, the School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, bullying or radicalisation. Further detail around the use of personal mobile devices can be found in the *Staff Acceptable Use Agreement*.

Information Security, Access Management and Cyber Security

The school makes every effort to maintain and improve the security framework around its devices, systems, services, accounts and data. We regularly review the effectiveness of these technology measures and procedures around them in order to keep up with the evolving cyber threat landscape. As part of Dukes Education Group we follow a recognised framework to improve the schools overall cyber security stance and lower the risk to our data, systems and people. This framework focuses on the following core risk control areas:

- Inventory and control of hardware, software and online assets
- Data protection (refer to the school *Data Protection Policy*)
- Secure configuration of hardware, software and online assets
- Account management
- Access control management
- Vulnerability management and patching
- Audit log management
- Email and browser protections
- Malware defences
- Backup and data recovery
- Network and infrastructure management
- Security awareness and skills training
- Service provider management
- Incident response management

Reporting Concerns & Complaints Handling

Concerns related to any aspect of digital and online safety should first be reported to the **Designated Safeguarding Lead (or a deputy)**. Any concern regarding a member of staff will always be reported to the Head. All reports will be treated with confidentiality and investigated promptly in line with our safeguarding procedures.

The school will take all reasonable precautions to ensure pupils and staff remain safe when using digital devices and when online. However, owing to the scale and complexity of the online world, the ways to connect and the speed of adoption and change, it is not possible to guarantee that children will always be protected from accessing unsuitable or harmful content. Neither the school, nor the school's owners, governors, directors, employees or contractors can accept liability for any materials accessed, nor any consequence that may arise from its access.

Staff and pupils are given information about infringements to this policy and the possible interventions or sanctions.

Complaints of cyber-bullying are dealt with in accordance with our *Anti-Bullying Policy*. Complaints related to child protection are dealt with in accordance with school's safeguarding procedures and *Complaints Policy*.

Reviewed by: Domingo Banesco Perez(Head)

Date: September 2026

Updated by: Paula O'Hara (eSafety Officer) September 2026

Reviewed by: Domingo Benasco Perez (DLS) September 2026

Approved by: Adam Anstey September 2026

This policy will be reviewed annually or in the event of changes in legislation, a significant change in technology provision or the environment in which the school operates