KNIGHTSBRIDGE SCHOOL

ICT & Online Safety Policy 2023-2024

This policy aims to promote a safe and secure digital environment and encourage positive behaviours for all members of our school community. 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 2023 (KCSiE 2023).

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

This policy should be understood in the context of other relevant school policies and procedures, especially the school *Safeguarding Child Protection Policy*, *Behaviour and Discipline Policy*, *Anti-Bullying Policy*, staff *Code of Conduct*, *Child on Child Abuse Policy*, *Policy for Distance Teaching and Learning;* the *Staff IT Acceptable Use Agreement*, the *Senior Pupil IT Acceptable Use Agreement* and the *Home-School Contract for the Safe use of The Internet and Digital Technologies*. It reflects the 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 the risk that some children have access to personal mobile networks (3,4 & 5G) and how this is managed at the 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 ICT systems, services or devices; on or off the school premises; including anyone accessing the school's ICT systems or services from non-school owned devices.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off school site and empowers staff to impose

disciplinary penalties for inappropriate behaviour. This is relevant to incidents of child-on-child abuse such as cyberbullying, and other online safety issues covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers in regard to searching for, and of, electronic devices and the deletion of offending data. In the case of both acts, action can only be taken over issues covered by the school's *Safeguarding Child Protection*, *Child-on-Child Abuse* and *Behaviour Policies*. The school will deal with such incidents within the scope of these policies and will, where known, inform parents/guardians of incidents of inappropriate online behaviour that take place out of school. The school also has responsibilities under the Counter Terrorism and Security Act (2015), commonly known as the Prevent Duty and measures in this policy are aligned with this.

Categories of Online Risks

KCSiE 2023 outlines four high level areas of online safety risk:

- Content: Being exposed to illegal, inappropriate, or harmful content
- Contact: Being subjected to harmful online interaction with other users
- Conduct: Personal online behaviour(s) that increase the likelihood of harm
- Commerce: Risks such as online gambling, inappropriate advertising, and phishing scams

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 systems that are regularly updated with threat intelligence to prevent access to illegal, inappropriate, or harmful content and monitoring systems that alerts relevant staff of behaviours that may be putting children at risk
- Contact and interaction: Measures are in place to monitor and minimise harmful online interactions including child-on-child risks such as cyberbullying, the sharing of explicit images and peer pressure; as well as risks typically posed by adults such as online grooming and radicalisation
- Conduct and online behaviour: The school teaches pupils and staff about responsible online behaviour, and highlights the risks, for example, of sharing explicit images, or engaging in online trolling, harassment or bullying
- Commercial risks: Online safety learning will include age appropriate content covering risks such as those posed by the inappropriate sharing of personal data or images; engaging with in-game purchases, online gambling or online scams; and infringing others' intellectual property

As a consequence of the rapid pace of i) new technologies being made available at low cost, and ii) development in online social and cultural trends, new risks and harms emerge quickly. To address this the school adopts a school wide approach that at least annually:

- Delivers up to date digital and online safety learning as part of the ICT curriculum and has a whole school approach that integrates learning opportunities across the curriculum

- Provides up to date ICT and online safety training (including cyber security & data protection) to all staff
- Assesses the provisions in place for filtering and monitoring of online content and the processes for managing and reporting of alerts and infringements
- Reviews technology, social and online trends to ensure the school's policies & procedures, technical measures, training, and curriculum are updated to reflect the current risks most pertinent to pupils, staff and the wider school community.

The current IT and online 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
- Hijacking 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 or elicit a reactive response

Roles and responsibilities

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
- Ensure that all governors / directors receive appropriate safeguarding & child protection training, including online at induction and regularly updated

- Are fully informed of the school's duty in regard of the UK Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) especially to process 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)

Are responsible for ensuring that:

- This policy is implemented and reviewed at least every year
- The procedures are in place so all staff understand and carry out their ICT 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 the UK Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), 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 reviews of i) this policy; ii) the staff ICT and online safety training; iii) the online filtering and monitoring provisions; and iv) the prevailing ICT and online safety risks assessment, to ensure the relevant staff and external providers meet our own high standards and legal commitments.

Senior Management Team (SMT)

- 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 the UK Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) 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 (and deputies), the eSafety Officer, while reporting to the SLT 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 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 and cyberbullying between pupils

Designated safeguarding lead (DSL) and deputies

- Takes lead responsibility for safeguarding and child protection including having oversight of the all online safety procedures and a good understanding of the filtering and monitoring systems in place at the school
- Liaise and support the school's eSafety Officer, SMT, IT team, and all relevant staff in matters related to safeguarding children in the physical, digital and online environments while reporting to the SLT and Safeguarding Governor in 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 the lead responsibility for all digital and online safety issues across the school
- Has the primary role in preparing updating and reviewing this *ICT & Online Safety Policy*; the staff and the senior 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 technical provision for filtering and monitoring
- Ensures that all pupils are aware of the expectations documented in the age appropriate Senior Pupil Acceptable Use Agreement and the *Home-School Contract for the Safe use of The Internet and Digital Technologies* and with the support from Heads of Sections (EYFS, Junior & Senior) maintains the records of pupil (and parental) agreement to them
- Is responsible for organising and delivering digital and online safety training as well as providing advice to staff, children and parents on these matters
- Make sure all staff have reviewed this IT & Online Safety Policy and the Staff IT Acceptable Use Policy and with the support of HR maintains the records of agreement to them
- Takes the lead role, and liases and advises the Designated Safeguarding Lead (and deputies), in all matters concerning digital and online safety
- Ensures that all children are taught how to keep themselves and others safe when using technology and 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 on all other relevant digital and online safety and cyber security matters
- Takes a proactive role in responding to filtering and monitoring alerts; analyses trends and reports these regularly to SMT / 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 SMT, 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

- Are Responsible for the running, maintenance & updates of filtering, monitoring and alerting systems
- Take 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
- Provide assistance to the DSL and deputies, the eSafety Officer, SMT 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
- 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), that encrypted copies of these 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
- Makes sure all staff members access to school systems is secured with unique credentials and protection is further enhanced with multi-factor authentication (MFA) wherever possible, especially for staff access to email and privileged systems administrator access
- Deploy and maintain and monitor an end-point detection and response (EDR) system on all 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 in class and reporting all instances where inappropriate content gets through the web filter.

All staff

- Must take responsibility to be familiar with this policy and read through, understand and agree to the Staff IT Acceptable Use Policy. If there is anything you do not understand you must seek help from the eSafety Officer.
- 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 and when online
- Attend and complete regular up to date safeguarding, online safety training, including all cyber-security and data privacy training.

Further, all staff should 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, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Pupils

- Be open to learn about and adopt good digital and online safety practices and show this in how you use technology and 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
- Pupil ICT and online Acceptable use Agreements:
    - For Reception and junior school pupils (Years 1-6) - your school planners have a page explaining "how we stay safe when using computers"
    - For Senior pupils (Years 7-11) - you will be asked to complete an online form at the start of each academic year (or when you join the school)

  For all pupils, i) you will be inducted in the safe use of devices and online at the start of each year, and ii) your parents and guardians will receive a copy of the *Home-School Contract for the Safe use of the Internet and Digital Technologies* and are asked to agree to uphold the same standards at home as we do so at school.

Parents and guardians

- Familiarise and agree to the schools *Home-School Contract for the Safe use of The Internet and Digital Technologies* 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 2023
- 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

Note that the school website, parent portal or any other school system that is made available to parents is done so in accordance with the specific Terms & Conditions and Privacy Policy published for each service.

External individuals and contractors

That require access to the schools ICT systems in order to carry out their duties on behalf of the school must first obtain approval from the eSafety Officer and agree to the Staff IT Acceptable Use Agreement.

Filtering & monitoring

- The school has appropriate filtering and monitoring systems in place and reviews their effectiveness each year.
- 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
- 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 DfEs Filtering & Monitoring Standards, this school:

- Has assigned roles and responsibilities to manage filtering and monitoring:
    - the IT team are responsible for the setup, maintenance and management of the systems, including liaising with technology suppliers, and play a supporting role in responding to alerts
    - the DSL (and deputies) take the lead role in responding to filtering and monitoring alerts, regularly reporting trends to SMT / SLT and Safeguarding Governor; and liaising with the IT team to ensure the systems are working effectively
    - the E-Safety Officer takes a supporting role in responding to filtering and monitoring alerts.
    - 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
- Has monitoring strategies in place to help meet our safeguarding responsibilities. These include i) physical monitoring by teachers and teaching assistants watching the screens of pupils; ii) a live supervision console using device management software in the IT room; iii) monitoring of network traffic and online activities; and iv) 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

We acknowledge the risk that some pupils may have access to personal mobile networks and unfiltered internet access while in school and this un-filtered and un-monitored activity can lead to inappropriate material and behaviour on the school premises. In response, this school does not allow the use of personal mobile or non-school managed devices by children while in school. 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).
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 appropriate acceptable use agreement or in the *Home-School Contract for the Safe use of The Internet and Digital Technologies*.

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.

The school will take all reasonable precautions to ensure pupils and staff remain safe when using devices and 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, the schools directors, employees or contractors can accept liability for all materials accessed, or 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 in the appropriate acceptable use agreement or the *Home-School Contract for the Safe use of The Internet and Digital Technologies*.

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*.

Prepared by: Simon Harrison (IT Consultant) September 2023

Reviewed by: Shona Colaço (Head) September 2023

Approved by: Aatif Hassan September 2023

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