KING'S HOUSE SCHOOL

RICHMOND

INTERNET SAFETY POLICY

Member of staff responsible:	Designated Safeguarding Lead
	Network Manager
Date of policy review:	January 2026
Date of next review:	January 2027
Approved by Governors:	January 2026

This policy applies to the whole school including the EYFS.

BACKGROUND

King's House School recognises that technology has transformed the lives of children and young people today, providing them with enormous opportunities to communicate, learn, research and play.

The School seeks to ensure that pupils have a positive experience of technology and appreciate its relevance in our society. The School wants the use of technology to be presented as a creative and fascinating process in which pupils are encouraged to use their own initiative, imagination, reasoning and investigative skills. The School expects all its pupils to become thoughtful users of technology and the internet and develop these capabilities to the best of their ability.

The School recognises that although IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, they also pose greater and more subtle risks to young people. The pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, cyber-bullying, harassment, grooming, stalking, abuse and radicalisation.

POLICY AIMS

This policy is intended to help us all think about the responsible use of technology and decide on the right balance between controlling access, setting rules and educating for responsible use. It covers:

- Guided educational use
- Risks and Safeguards
- Reporting Issues and Concerns
- Child Protection and Safeguarding
- Safe Use of the internet at Home

This policy should be read in conjunction with the following School policies: Staff IT Acceptable Use, Student Chromebook Acceptable Use, Artificial Intelligence, Safeguarding and Anti-Bullying.

GUIDED EDUCATIONAL USE

The purpose of internet use in the School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management information and business administration systems. Internet use is a part of the statutory curriculum

and the School has a duty to provide pupils with quality internet access as part of their learning experience.

Pupil access to the School internet is designed expressly for pupil use. Teachers guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity. Aimless surfing is not permitted. Specialist applications are integrated into the curriculum to stimulate discussion, promote creativity and enhance and extend learning. The School reinforces this through our WARL expectations (Websites and Applications that are Relevant to the Lesson), which are in place to help maintain a focused and respectful learning environment for all pupils.

The School educates pupils in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation as well as respect for copyright. They are taught what internet use is, and is not, acceptable and how to manage their own online profile in such a way to avoid future embarrassment.

RISKS AND SAFEGUARDS

The internet is available to all through a variety of communication devices. Anyone can send messages, discuss ideas and publish material with little restriction. These features make it both an invaluable resource used by billions of people every day, as well as a potential risk to young and vulnerable people.

All staff are made aware of the School's expectations regarding their use of School ICT systems, the internet, iPads, mobile phones and camera devices. Staff development in safe and responsible internet use is provided as necessary.

To support a safe and purposeful learning environment, all members of staff must take responsibility for verifying the suitability of any online resources they intend to share with pupils. This includes evaluating the educational relevance, age-appropriateness, and safeguarding implications of any external content. Websites must be checked for inappropriate advertising, unmoderated user content, embedded links, and any risk to pupil data or wellbeing. Where there is any uncertainty about a website's suitability, staff must seek guidance from the Network Manager, Head of Digital Learning or Designated Safeguarding Lead before sharing it with pupils. This process forms part of the School's broader duty to protect pupils from potentially harmful online content and aligns with our Staff IT Acceptable Use, Safeguarding and Online Safety policies. All website usage must reflect the School's ethos of responsible and respectful use of technology.

Technical Infrastructure & Safeguards

All computers at the School are connected to the internet, across which a range of services (including cloud services) are provided to users of the School network. All pupils are issued with their own personal logins for use on the School's network. Access is via a personal login, which is password protected. Where submitted electronically, all school work, assignments and research projects should be submitted using Google Classroom. Pupils should be aware that all activity using the School networks is logged.

The School's Network Manager works to ensure that the IT infrastructure is not open to misuse or malicious attack and that all protection software is up-to-date. All network access is password protected and all users have clearly defined access rights in accordance with their role. The School systems are reviewed regularly with regards to security.

An important part of the School's role is to protect pupils from accessing potentially harmful content on the internet. Much of the material is published for an adult audience and some is unsuitable for pupils. The School will do all it reasonably can to limit pupil's exposure to pornographic, terrorist and extremist material by having in place appropriate filters and monitoring systems which are designed to protect children from harmful content without "overblocking" or imposing unreasonable restrictions as to what children can be taught through online education. Access levels are regularly reviewed to reflect the curriculum requirements and age of pupils.

Access to specific software is determined by the teaching staff and implemented and monitored by the Network Manager. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted.

Staff will conduct a level of in-person monitoring if they are in a room with students on devices, as part of wider classroom supervision. In-person monitoring will be supported by technical monitoring systems which allows teachers to monitor pupils' Chromebook screens in real time and further logs all web usage and typed content. Weekly monitoring reports highlighting incidents are sent to the relevant school staff. An immediate report is produced when an incident is classed as high-risk, for example, of malicious, technical or safeguarding nature.

Internet Safety

In a perfect world, inappropriate material would not be visible to pupils using the internet, but this is not easy to achieve and cannot be guaranteed. 21st century life presents dangers from which

children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become "Internet Wise".

Age appropriate lessons are given in both Computing and PSHE about the dangers of the internet and mobile devices.

Pupils are not permitted to access social networking sites at the School (users should be 13 years+) but the School teaches the safe use of social networking sites as it is aware that some pupils do use them outside school.

Pupils are taught how they can avoid making themselves vulnerable to a range of risks including identity theft, cyber-bullying, abuse, grooming and radicalisation.

Cyber-bullying & Sharing of Nude and Semi-nude Images (Sexting)

Pupils may use technology (social websites, mobile phones, text messaging, photographs and email) to abuse other pupils. This is most likely to take the form of cyber-bullying but may also include the consensual and non-consensual sharing of nude and semi-nude images and/or videos. These are aggressive, nasty and intentional acts against a victim who cannot easily defend themselves.

The School uses lessons and assemblies to help children understand, in an age-appropriate way, what abuse is. Pupils are taught about the responsible and safe use of social media in Computing and PSHE lessons. They are taught that it is a criminal offence to send an electronic communication (words and/or images) to another person with the specific intent to cause distress or anxiety, and are encouraged to report any incidents immediately to their parents or a teacher.

If the School discovers that a pupil is being subjected to cyber-bullying, it will be dealt with through the procedures detailed in the School's Anti-Bullying Policy. If staff become aware of a sexting incident, it will be reported to the School's Designated Safeguarding Lead (DSL).

Smart/Mobile/Camera devices

Only Year 5 to Year 8 pupils are permitted to bring a mobile phone into school, for safety purposes when travelling independently to and from school. However, pupils in Years 5 and 6 are not permitted to bring smartphones. Year 7 and 8 pupils are encouraged to bring non-smart (brick) phones. All mobile phones must be switched off when entering the School and handed in to the school on arrival. They will then be kept securely on site and collected by pupils at the end of the day. Pupils who leave directly from the grounds following afternoon games will be given their

devices by a member of the PE Department. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. We would request that pupils refrain from wearing these devices.

Pupils who bring personal electronic devices, including mobile phones and smartwatches, do so at their own risk. The School does not accept responsibility for the loss, theft or damage of such items.

Visitors may only use their own smart/mobile devices in the reception area and for recording their child's performance in an assembly or school production in the theatre, subject to the restrictions set out in the School's Taking and Storing Images of Children Policy. The use of camera devices of any sort is not permitted in toilets, washrooms or changing areas.

Tracking/Recording Devices

Pupils may bring a tracking device into school and on school trips. These devices should be kept in the child's pocket or bag and should not disrupt the school day. Any kind of device with the purpose of recording audio is not permitted in school and will be turned off if found.

School Website

The contact details on the website are the School address, e-mail and telephone number. Personal contact details for staff will not be published. Images that include pupils are selected carefully and pupils' full names will not be used in association with photographs or content without consent.

Parents may advise the School in writing if they do not permit the School to publish images of their child. The Head takes overall editorial responsibility and ensures that content is accurate and appropriate.

REPORTING ISSUES AND CONCERNS

Despite all attempts at filtering, pupils may occasionally be confronted with inappropriate material. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: if they are using the internet they should close the page and report the incident immediately to the teacher.

Any inappropriate content access that is identified by the School monitoring systems will be reported by the School's Network Manager and any incidents of misuse will be investigated. Staff

will report any inappropriate content that gets through the filtering system to the Network Manager who will ensure it is immediately blocked.

It is hoped that all members of the School community will understand and follow this policy. However, there may be times when infringements could take place, through careless or irresponsible or, very rarely, deliberate misuse. In such cases:

- A child can report the incident to a teacher
- A teacher can report the incident to a member of the SLT
- A parent can report the incident to the Form Teacher or the Head
- The Head can report the incident to the Chair of Governors

Any concern or complaint about staff misuse must be referred to the Head, unless it is the Head in which case the referral must be made to the Chair of Governors.

CHILD PROTECTION AND SAFEGUARDING

Any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers will be referred to the Police.

If we discover that a pupil is at risk as a consequence of online activity, it will be treated as a Safeguarding matter. Should a high-risk safeguarding incident be reported by the monitoring system, an alert shall be sent to each member of the DSL team as well as the Network Manager and IT Technician to ensure the alert reaches the DSL, or in their absence, a DDSL. The School will seek assistance from the appropriate authorities such as the Child Exploitation and On-line Protection Unit (CEOP), the police and/or Richmond Local Safeguarding Board. The School's Safeguarding procedures are detailed in the School Safeguarding Policy.

CEOP (Child Exploitation & On-line Protection Centre)

The National Crime Agency's CEOP Command (www.ceop.gov.uk) works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account.

Their website, www.thinkuknow.co.uk, contains internet safety advice for children, parents and teachers.

When using School devices or networks at home, out of school hours, the School will do all it reasonably can to respond to high risk alerts, however, it cannot be held responsible for a pupil's actions if any monitoring alerts are not reviewed straightaway.

The School conducts an annual online safety review as laid out by Keeping Children Safe in Education (KCSIE), which allows the School to evaluate and update online safety strategies as well as identify technical limitations. This review involves an annual risk assessment of evolving online threats, a review of filtering and monitoring systems, and integration with broader safeguarding reviews to ensure a comprehensive, whole-school approach to protecting children online.

SAFE USE OF THE INTERNET AT HOME

At home, sometimes children can be given unsupervised access to the internet. This, potentially, allows them to access all kinds of society and materials. The School believes that by fostering a sensible approach at home and at school, it will be able to equip children with the skills they need to become responsible users of technology and help protect them from harm. In the Senior Department, homework is set via Google classroom. Parents are encouraged to discuss with their child the sites that they may be required or wish to access as part of their homework.

The School asks parents to consider:

- Prohibiting the use of social networking sites under the age of 13.
- Talking to their child about what they are doing on-line and, if possible, restrict their computer use to a shared area at home so they can be aware of sites that are being accessed.
- Ensuring their child does not give out any personal details of any kind which may identify them (including telephone numbers and addresses) to people they may meet online, including on games consoles.
- Ensuring that appropriate content filters are switched on.
- Encouraging the use of search engines designed specifically for children such as Safe Search Kids or Swiggle or by ensuring Google Safe Search is switched on.

PARENT CONCERNS

If parents have concerns about any of the subjects raised in this policy, they should contact the Head or Bursar who are responsible for ensuring compliance with this policy.