TKS E-Safety Policy

Written by:	MC/TO	Date:	November 2021
Most recently updated by:	RG	Date:	July 2024
Approved by:	APS	Date:	July 2024
Review frequency:	Bi-annual	Date of next review:	July 2026

CONTENTS

1. Introduction

The King's School is committed to a policy of protecting the rights and privacy of all individuals. To do this we need to collect and use certain types of data to fulfil our commitments to our staff, pupils and volunteers. This personal information is collected and processed appropriately in accordance with the TKS Data Protection Policies. This policy outlines how we protect personal data and seek to keep safe online. All staff, pupils and volunteers of The King's School who have access to personal information will be expected to comply with this policy.

2. This Document

This document is in 2 sections.

1. The TKS E-Safety Policy (Part 1) - this document, includes the policy details
2. The TKS E-Safety Policy (Part 2) - this section is a compilation of the acceptable use agreements and permission forms that require signing by various users

3. Scope of the Policy

This policy applies to all members of The King's School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of The King's School's digital technology systems, both in and out of The King's School.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off The King's School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of The King's School, but is linked to membership of The King's School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). The King's School will deal with such incidents within the guidelines included in this policy as well as in the associated behaviour and anti-bullying policies. The King's School will also inform parents/carers of reported incidents of inappropriate online behaviour that occur outside of the school premises.

4. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within The King's School. Some of the roles described below may be combined.

a. Governors

- Governors are responsible for the approval of The TKS E-Safety Policy and for reviewing the effectiveness of the policy.
- The TKS E-Safety Policy is an integral part of the wider Safeguarding Policy. Monitoring will be carried out by the Governors receiving regular Safeguarding reports.

b. Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for The TKS E-Safety Policy will be delegated to the DSL, IT technician and teachers.
- The Principal, Heads and the DSL should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is the same process as the Complaints Policy.

c. Data Protection Officer (DPO) – SchoolPro TLC

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing The King's School online safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides regular training and advice for staff.
- Liaises with the Information Commissioner's Office (ICO) and relevant bodies.

d. IT Technician/ Team

The King's School use an ICT provider: Active IT (Active IT Solutions) for server-side support. The onsite support is managed from the school by the IT technician.

The IT technician is responsible for ensuring:

- The King's School's technical infrastructure is secure and is not open to misuse or malicious attack.

- The King's School meets required online safety technical requirements and any ICO, Local Authority or other relevant body e-safety policies or guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis (in association with Active IT).
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Review online browsing reports to understand pupil and staff activity.
- Internet browsing is regularly monitored for 'activity' based behaviour and appropriate action taken regarding non-compliance.

e. Teaching and Support Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current TKS E-Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).
- They report any suspected misuse or problem to the Principle, DPO and IT Technician for investigation / action / sanction.
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official The King's School systems or user accounts.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow The TKS E-Safety Policy and the Acceptable Use Policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

f. Designated Safeguarding Lead (DSL)

E-Safety, including filtering and monitoring, comes under the umbrella of safeguarding and the DSL has responsibility for online incidents across the school. The DSL should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online-bullying

All Safeguarding training should also include e-safety.

g. Pupils

- are responsible for using The King's School digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- are expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking / use of images and on online bullying.

- should understand the importance of adopting good online safety practice when using digital technologies outside of The King's School and realise that The TKS E-Safety Policy covers their actions out of The King's School, if related to their membership of The King's School.

h. Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The King's School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters/emails, the School website / learning platformand other means of providing information about helpful websites and national / local online safety campaigns / literature. Parents and carers will be encouraged to support The King's School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at The King's School events;
- access to parents' sections of the website / learning platform and on-line pupil records; and,
- their children's personal devices in The King's School (where this is allowed).

i. Community Users/ Hirers

Hirers are only given access to the New Yatt Road WIFI network which ensures their physical separation to the school's data servers, so no further action is required to secure the data.
A content management technology is in use at the boundary firewall to reduce the risk by restricting access to inappropriate web content.

5. Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of The King's School's online safety provision. Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum as part of the PSHE curriculum which is regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
    - The Counter Terrorism and Securities Act requires The King's School to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside The King's School.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can

temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

6. Education – Parents and Carers

Some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The King's School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, website, learning platform;
- Parents / Carers training sessions; and,
- Individual consultations where applicable.

7. Education & Training – Staff and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety is included in safeguarding training and safeguarding staff updates / refresher sessions.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand The TKS E-Safety Policy and Acceptable Use Agreements.
- The DSL (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- Any significant updates to The TKS E-Safety Policy will be presented to and discussed by staff in staff / team meetings.

8. Training – Governors

Governorsreceive online safety training as part of their safeguarding training. They are also trained on Prevent awareness. This is of particular importance for those who are members of any subcommittee / group involved in technology / online safety / /safeguarding. This may be offered in a number of ways:

- Attendance at external training opportunities where available;
- Participation in The King's School Safeguarding training or information sessions for staff or parents.

9. Technical – infrastructure / equipment, filtering and monitoring

The King's School has a managed ICT service provided by an outside contractor; it is the responsibility of The King's School to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of The King's School, as suggested below. It is also important that the managed service provider is fully aware of The TKS E-Safety Policy and the Acceptable Use Agreement.

The King's School is responsible for ensuring that The King's School infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also ensures that the relevant people named in the above sections are effective in carrying out their online safety responsibilities:

- The King's School technical systems will be managed in ways that ensure that it meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to technical systems and devices.

- All users (at KS2 and above) will be provided with a username and secure password by the IT technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
  Note: All users of the network are allocated usernames with complex passwords
- The "master / administrator" passwords for The King's School ICT systems, used by the IT technician/ team (or another person) must also be kept in an accessible secure place. (This is kept by both the outsourced ICT partner and in the IT Administration Guide (password protected).
- The IT Technician is responsible for ensuring that software licences are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. (Inadequate licencing could cause The King's School to breach the Copyright Act which could result in fines or unexpected licensing costs).
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. NB. additional duties for The King's School under the Counter Terrorism and Securities Act 2015 which requires The King's School to ensure that children are safe from terrorist and extremist material on the internet
- An appropriate system is in place (through the class tutor system) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of The King's School's systems and data. These are tested regularly. The King's School's infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (see Acceptable Use Agreement) that forbids staff from downloading executable files and installing programmes on The King's School's devices.

10. Removable Media (staff only)

With many methods of secure data transfer, The King's School does not use removable media. Only in exceptional circumstances will removable media be used. This must be provided by the IT department and this needs to be encrypted and/or password protected.
It is also imperative that any data is not stored longer than necessary and deleted afterwards in compliance with the data retention and Disposal Policy.
We do have several caveats to the policy. These are:

1. This does not apply to camera removable media as it is currently not possible to encrypt camera memory cards. In this situation, alternative secure methods must be used. Speak to the IT support team.
2. In the exceptional situations that removable media devices are required (e.g. bulk transfer of video footage) the IT department will provide an appropriate secure solution (e.g. encrypted external drive, secure shared cloud based storage).
3. USB devices used with photocopiers are acceptable (as they are a reduced risk).
4. USB devices are used for coursework and exams but data is removed in a timely manner.

IMPORTANT - Any removable media that is introduced into the school network MUST be scanned for viruses before any file copying is done. Ask IT Support on how this simple task is done.

11. Mobile Technologies (including 'Bring Your Own Device')

Mobile technology devices may be The King's School owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilizing

a network. Own devices must connect through The King's School network to ensure filtering and monitoring is in place. Devices are set up by the IT technician.

All users should understand that the primary purpose of the use of mobile / personal devices in The King's School context is educational. This policy should be consistent with and inter-related to other relevant King's School polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of The King's School's education programme.

- The King's School's Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies.

12. Use of digital and video images

- The new pupil forms (including the acceptable use form) explicitly asks parents, when they join the school, to allow/disallow photographs of their children to be posted. These are for several scenarios
    - Internal education use (classroom, Art etc)
    - Managed School promotional use (open days etc)
    - External public use (website etc)

- When using digital images, staff inform and educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at The King's School events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims but must follow The King's School policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; staff personal equipment should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or The King's School into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission within school time.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs.

13. Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR) announced in 2016. As a result, The King's School is subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the appendices to this document. The King's School will ensure that it takes account of policies and guidance provided by local authorities or other relevant bodies. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Staff must ensure that they:

At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Any files that need to be sent to parents containing personal or sensitive information must be sent as a password protected link. Subject lines of titles of files should not contain personal information.

14. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how The King's School currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technology	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to The King's School	x					X		
Use of mobile phones in lessons		x					X	
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices		x					x	
Use of personal email addresses in The King's School, or on The King's School network		x						x
Use of The King's School email for personal emails				X				x
Use of messaging apps		x						x
Use of social media		x						x

Use of blogs		x						x

When using communication technologies, The King's School considers the following as good practice:

- The official King's School email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only The King's School email service to communicate with staff when in The King's School, or on The King's School systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with The King's School policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content**.** These communications may only take place on official (monitored) The King's School systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are taught strategies to deal with inappropriate communications and reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on The King's School website and only official email addresses are used to identify members of staff.

15. Social Media - Protecting Professional Identity

The King's School has a duty of care to provide a safe learning environment for pupils and staff. The King's School could be held indirectly responsible for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render The King's School liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The King's School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and The King's School through:

- Training that supports and promotes GDPR principles;
- Ensuring that personal information is not published;
- Recruiting staff following Safer Recruitment guidelines;
- Clear reporting guidance, including responsibilities, procedures and sanctions; and,
- Risk assessment, including legal risk.

The King's School staff ensures that:

- No reference is made in social media to pupils, parents/carers or other school staff;
- They do not engage in online discussion on personal matters relating to members of The King's School community;
- Personal opinions are not attributed to The King's School;
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information;

When official social media accounts are established for The King's School, there is:

- A process for approval by senior leaders;
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
- A code of behaviour for users of the accounts.=;

- Systems for reporting and dealing with abuse and misuse; and,
- Understanding of how incidents may be dealt with under The King's School disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with The King's School or impacts on The King's School, it must be made clear that the member of staff is not communicating on behalf of The King's School with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon The King's School are outside the scope of this policy.
- Where excessive personal use of social media in The King's School is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The King's School permits reasonable and appropriate access to private social media sites.

16. TKS Safeguarding Policy - Home Learning

The following details good safeguarding practice for Home Learning in the event of an enforced School buildings closure where remote learning is offered. This serves as additional guidance beyond that already stated in the policy.

The Prevent Duty and all other basic safeguarding approaches should always be applied. Please contact the DSL (Designated Safeguarding Lead) team via email or phone, to report any concerns which arise while using online platforms in the event of enforced school buildings closure.

17. General online safety guidelines

- Staff should only use TKS approved online platforms that are currently used for School purposes for communicating and running online learning.
- Staff should only use TKS email addresses.
- Staff should have full confidence that the parent or carer is aware of the online activity. This is ensured through a parent/carer approved email confirmation.
- Staff should ensure the background to any video conferencing is neutral and does not show any inappropriate images or documentation. We recommend pupils participate in remote learning from a communal area (lounge, kitchen etc) but we understand this is not necessarily possible.
- Staff should ensure communications with a pupil remain professional in the same manner they would in school.
- Staff should report any inappropriate activity or incident to the DSL.
- Pupils should report any concerns to parents or call the school number and ask to speak to the DSL.
- Pupils should have a responsible adult nearby when sessions are taking place, and/or have received permission from their parent for the teaching session to take place.
- Pastoral provision remains a priority for students even in the event of a school buildings closure; staff should refer any concerns they have to the pastoral leads in the way they would in school. It remains the role of the teacher to look out for the wellbeing of pupils they are teaching.
- If a member of staff is NOT hosting/participating in the call, pupils should not use the TKS Remote Learning capability.
- Parents and pupils should not share log on details.
- Parents and children should not take screen shots or photos of other children on-line on personal devices.

The school is aware that pupils will be spending more time online when home learning is enforced, therefore staff will be mindful of the need to promote safe online usage when teaching using online platforms.

18. Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from The King's School and all its technical systems. Other activities (e.g. cyber-bullying) are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a The King's School context, either because of the age of the users or the nature of those activities.

The King's School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside The King's School when using The King's School equipment or systems. The King's School policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm					X
	Promotion of extremism or terrorism					X

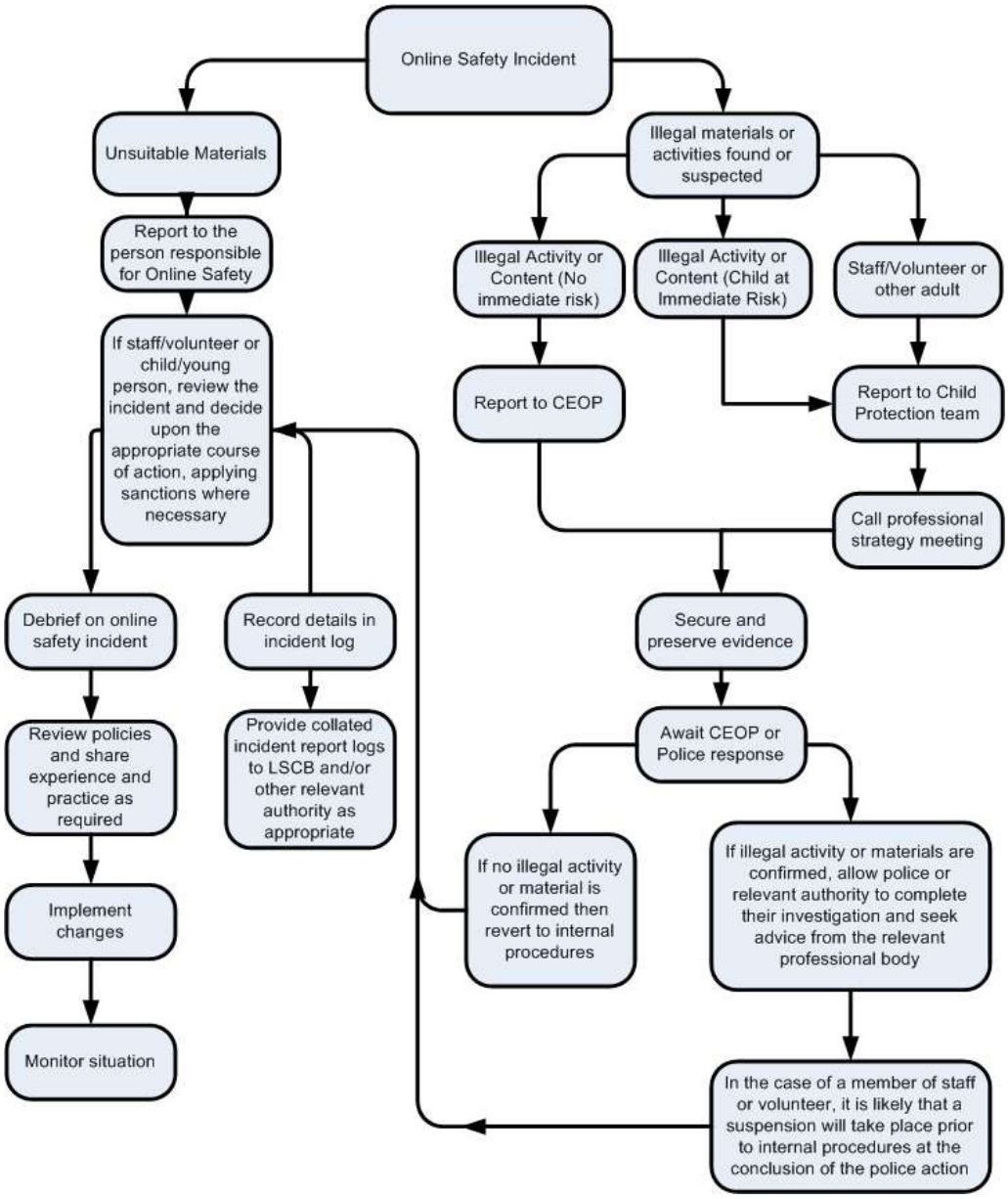
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of The King's School or brings The King's School into disrepute				X	
Using the King's School systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by The King's School					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing			x			
Use of social media			X			
Use of messaging apps			x			
Use of video broadcasting e.g. You Tube			X			

19. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

20. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



21. Other Incidents

It is hoped that all members of The King's School community will be responsible users of digital technologies, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and, if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority group or national / local organisation (as relevant).
    - Police involvement and/or action

- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for The King's School and possibly the police, and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

22. The King's School Actions & Sanctions

It is more likely that The King's School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of The King's School community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the Behaviour, Suspensions and Exclusions Policy and through the Staff Code of Conduct and Staff Discipline Policy.