KINGS' SCHOOL

ONLINE SAFETY POLICY

Policy Reviewed by:	SLT	Jan 2018
Approved by:	Pupil Support Committee	Mar 2018
Endorsed by:	FGB	Mar 2018
To be Reviewed	3 Yearly	Mar 2021

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by:

- Designated Safeguarding Lead
- ICT Coordinator
- Senior Leadership Team
- School Governing Body

The school will monitor the impact of the policy using:

- Monitoring logs of internet and network activity (including sites visited) / filtering / Impero

Scope of the Policy

This policy applies to all members of Kings' School (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school site.

This policy must be read and understood alongside the school's Safeguarding Policy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Pupil Support and

Curriculum Committees receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of ICT Governor.

The role of the ICT Governor will include:

- regular meetings with the ICT Coordinator and ICT Strategic Lead
- reporting to relevant Governors Committees and Full Governing Body

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the ICT Strategic Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

ICT Strategic Lead:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy / 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 training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with ICT Governor to discuss current issues
- attends relevant Governor meetings
- reports regularly to Senior Leadership Team

ICT Co-ordinator:

- to create and implement a Whole School ICT Plan
- to lead innovation in the use of new technologies within classrooms
- to Chair BISCUIT/Strategic Group
- to co-ordinate 'ICT Tip of the Week'
- to liaise with SLT over the ICT Budget
- to monitor and review the ICT Managed Service contract (including canvassing staff for feedback)
- to attend ICT Performance Management Review Meetings with SLT
- to present ICT initiatives to SLT and other key users/stakeholders in school
- to visit and liaise with other schools in order to share good practice and expertise
- to develop and promote ICT Training in school
- to review Policies relating to ICT/Acceptable Use/ Online Safety
- to champion Online Safety

IT Support Manager / Technical staff:

The IT Support Manager/ Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (upstream by HSPN2 and internally by Flexible Web) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that 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
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / ICT

Strategic Lead / ICT Coordinator for proper investigation and subsequent action / sanction

- that monitoring software / systems are implemented and updated.

Teaching and Support Staff

School teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the Headteacher, DSL, Data Protection Officer and ICT Coordinator as appropriate for proper investigation and subsequent action / sanction
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems
- when working away from a logged on workstation – it is locked
- staff using mobile devices to check e-mails or access the network must have a complex security code (fingerprint, iris or 6 digit PIN) enabled on the device. School e-mail is only to be used for school business. Staff must not use their personal e-mail to conduct school business
- they have read the Online Safety policy
- pupils understand and follow the IT Rules and Code of Conduct for Internet use and emails in the pupil handbook
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations as stated in the pupil acceptable use agreement
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- they monitor use of pupils computers using Impero
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that they understand how to manage any unsuitable material that is found in internet searches through use of Impero and informing the ICT Coordinator

Staff laptops

- Laptops are issued to all teaching and some support staff. The issued laptop remains school property and should only be used by its designated keeper for school-related tasks

- School employees issued with laptops do not have any right to privacy as far as the content of school laptops is concerned and so it is absolutely essential that they are NEVER used for purposes inconsistent with the professional standards of school teachers and support staff.

- The school has a range of security software that will automatically detect and report inappropriate material. The school reserves the right to inspect all school computers and devices, including records of internet sites visited, emails and attachments and any material downloaded. Using any school computer or device inappropriately can be a disciplinary offence

- Staff should treat laptops as they would any other valuable items and ensure that appropriate security measures are taken. Laptops should not be left unattended at school or in vehicles and care should be taken to ensure that any sensitive data is kept secure to meet the requirements of the General Data Protection Regulations. It is the responsibility of the member of staff to take all reasonable steps to prevent unauthorised access to the laptop

- Staff should not add software to their laptop. Software must not be copied from the laptop to another device without permission from IT Support and ICT Coordinator. IT Support will carry out upgrades to software as required. Staff wishing to use subject specific software must liaise with IT Support to ensure that appropriate licences are held

- Staff will be required to sign for laptops and should be aware that this equipment will be audited regularly and on return to ensure that equipment has been used within the guidelines specified

Passwords

- Passwords must be complex (numbers and mix of symbols, upper and lower case).

- Passwords must not be divulged to others nor should they be kept in a place that someone could find them
- If a member of staff suspects their password has been compromised, they must inform IT Support and the ICT Coordinator.

Designated Safeguarding Lead (DSL)

DSLs are trained in Online Safety issues and are to be aware of the potential for serious child protection and safeguarding issues that arise from:

- sharing of sensitive personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- Sexting
- Taking / sharing of inappropriate material (images /videos)
- Issues arising from use of Social Media

Pupils

- are responsible for using the school computer equipment in accordance with the IT Rules, IT Code of Conduct and Parent / Pupil Contract contained in the Pupil Handbook.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand the school rules concerning the use of mobile devices and digital cameras.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet. computers and mobile devices in an appropriate way. The school will take

every opportunity to help parents understand these issues through Internet Safety presentations, signposting using the school website and in routine school communications. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school

Policy Statements

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 is therefore an essential part of the school's online safety provision. Pupils need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages. The online safety curriculum will be provided in the following ways:

- A planned online safety curriculum will be provided as part of BEE and PHSEE
- Key online safety messages are reinforced as part of a planned programme of assemblies
- pupils should be taught in all subjects to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils should be 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.
- pupils should be helped to understand the need for the IT Rules and IT Code of Conduct and encouraged to adopt safe and responsible use both within and outside school.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet

searches being blocked. In such a situation, staff can request that the ICT Strategic Lead / ICT Coordinator 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.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented.

School technical systems will be managed to deliver secure and safe use:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Access to the school's network systems will be restricted to designated users.
- All users will be provided with a username and secure password by IT Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at regular prescribed intervals.
- The passwords for the school ICT system, including the administrator passwords used by the IT Support staff will be held by the managed service provider and available to the Headteacher.
- IT Support Staff are responsible for ensuring that software licence logs 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
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the HSPN2 broadband and internally using Flexible Web filtering.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering allowing different filtering levels for staff and pupils

- IT Support staff regularly monitor and record the activity of users on the school network and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An Acceptable Use agreement is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems).
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (Use of USB Memory sticks or other removable media will not be permitted after 1 May 2018 without the written permission of the IT Coordinator)

Use of digital and video images

School staff, parents, carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents and carers are welcome to take videos and digital images of their children at 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 school policies concerning the sharing, distribution and publication

of those images. Those images should only be taken on school equipment; the personal equipment of staff 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 school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- 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 blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, the prospectus or news media
- Pupils' work can only be published with the permission of the pupil and parents or carers

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (to be replaced by the General Data Protection Regulations (GDPR) in May 2018). Detail is contained in the school's Data Protection Policy.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official 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 school email service to communicate with others when in school, or on school equipment(eg by remote access)

- Users must immediately report, to the nominated person – in accordance with the 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, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications. Members of staff who receive inappropriate communications from pupils MUST report them to their line manager immediately

• Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media - Protecting Professional Identity

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

- Ensuring that personal information is not published on social media
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- They do not post on social media any content which identifies pupils, parents, carers or staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Any personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

The school's website and any associated social media for professional purposes will be checked regularly to ensure compliance with the school's policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is not permitted on the school network or computer systems. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The 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 school when using school equipment or systems. The 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 school or brings the school into disrepute				X	
Using 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 school / academy					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (eg 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. Youtube				X		

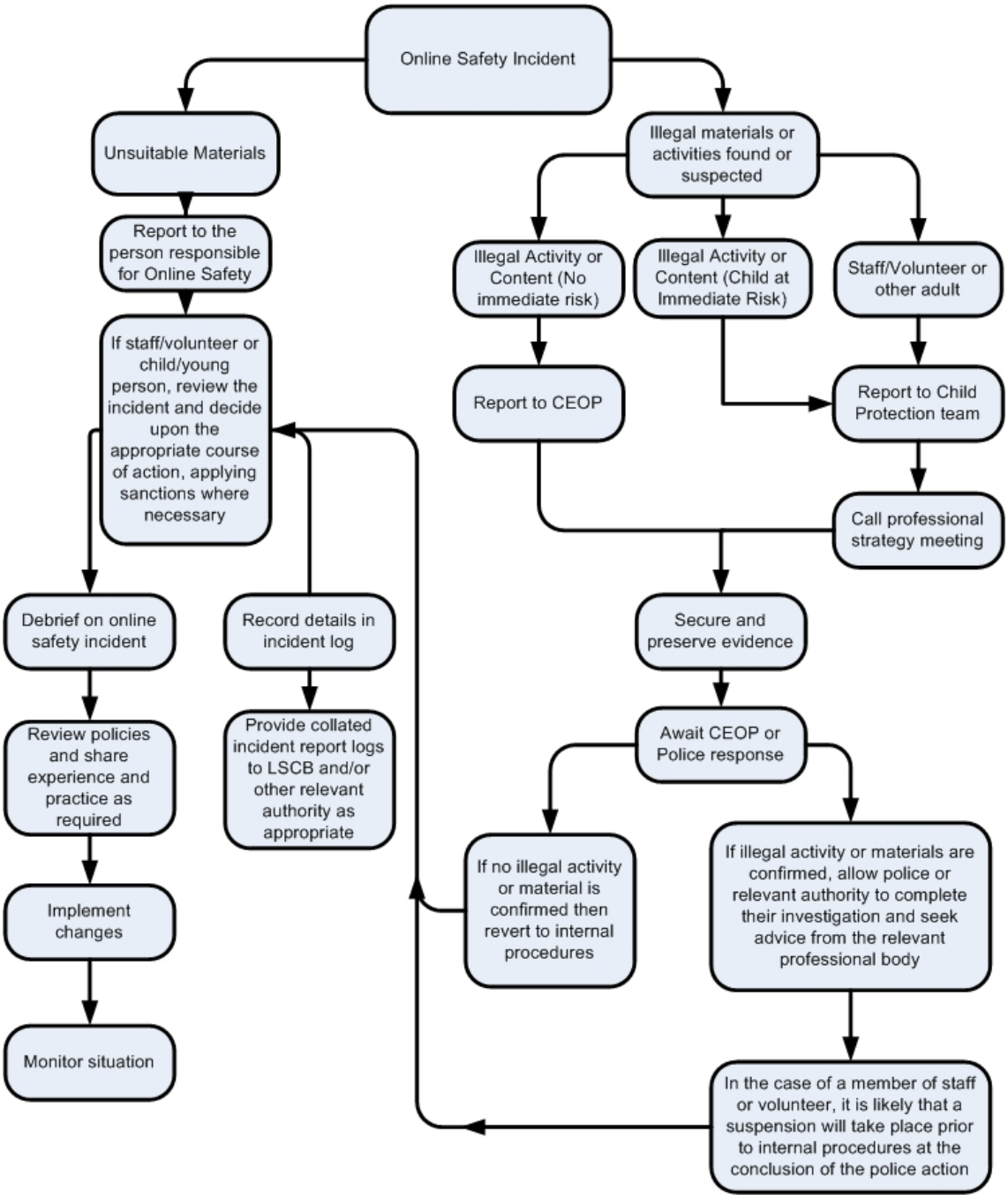
Responding to incidents of misuse

In the event of any suspicion that there has been misuse of the school's network or computer systems then the flowchart below should be used to determine the appropriate actions.

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.

If there is any concern about the behaviour of an adult, the Headteacher must also be informed. If the adult is the Headteacher, the Chair of Governors must also be informed.



Other Incidents

Any infringements of this Policy, through careless or irresponsible or deliberate misuse will be investigated using the procedure below:

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

- Have more than one senior member of staff involved in the investigative 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 to the members of staff conducting the investigation.
- 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 investigation report except in the case of illegal content – see below
- Once this has been completed and fully investigated the Headteacher 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
    - Police involvement
- **If content being reviewed includes images of Child abuse or other illegal content 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 or device under investigation. 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 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.