King's Schools
TAUNTON

Online Safety Policy

This policy is applicable to all pupils including those in EYFS

Responsibility

Individual: Network Manager / Designated Safeguarding Lead (Online Safety Co-ordinator) / Deputy Head Pastoral / Headmaster

Review

Last review date: May 2019

Next review date: May 2020

This policy should be read in conjunction with the following school policies:
Child Protection
Anti-bullying
Behaviour
IT Acceptable Use (see Staff Handbook)
Policy on creation and use of digital and other images of current pupils

INTRODUCTION

The development and expansion of the use of ICT, and particularly the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximize their potential use as a learning tool, but also to prepare themselves as life-long learners and for future employment. There is a large body of evidence that recognizes the benefits that ICT can bring to teaching and learning. King's Schools Taunton have made significant investment both financially and physically to ensure that these technologies are available to learners. The benefits are perceived to out-weigh the risks. However, through this online safety policy, we must ensure that we meet our statutory obligations to ensure that our children are safe and protected from potential harm both inside and outside our school.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to minimise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. Some of the dangers that may be faced include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- The risk of being subjected to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers (see Child Protection and Safeguarding policy)
- Sexting
- Radicalisation (see child protection and safeguarding policy)
- Online bullying (see anti-bullying policy)
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement

- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of a child/young person

At King's Schools Taunton, we understand the responsibility to educate our pupils regarding Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the School. This can make it more difficult for the School to use technology to benefit learners.

Everybody in the School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy, the IT Acceptable Use policy (in the King's Schools Taunton Ltd Staff Handbook and the Acceptable Use Agreement for pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

The Online safety policy that follows explains how we intend to provide the necessary safeguards to ensure that we have managed and taken steps to reduce the risks involved with this technology, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

SCOPE OF THIS POLICY

This policy applies to all members of the school community (including staff, children, support staff, parents, and visitors)

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

MONITORING

The implementation of this online safety policy will be monitored by the:	*SMT and ITSG*
Monitoring will take place at regular intervals:	*Annually*
The DHP will report to the council on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*May 2020*
Should serious online safety incidents take place, the following persons will be in charge:	*Designated Safeguarding Lead in liaison with the Head.*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Internal monitoring data for network activity*

ICT Support department and /or other authorised employees will undertake inspections of any ICT equipment owned or leased by the School or attached to the school network at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law.

Staff should read and be familiar with the guidelines as set out in the Staff Handbook.

ROLES AND RESPONSIBILITIES

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

Headmaster and SMT

- The Headmaster is responsible 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 Online Safety Co-ordinator
- The Headmaster / SMT are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. WRAP training is an essential part of this process in both schools
- The Headmaster / SMT 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. The SMT will receive regular monitoring reports from the Online Safety Co-ordinator
- The Headmaster 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 SWGfL flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures). In the event of an incident involving material of a radicalisation nature, the Prevent team will be contacted directly by the DSL/Headmaster

Online Safety Coordinator (this will be the DSL/ DDSL at each school unless otherwise agreed)

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the 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
- is particularly sensitive to the threat of Radicalisation and provides training and support to all staff within this area
- provides training and advice for staff
- liaises with the Local Authority (Safeguarding, Prevent etc)
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- attends relevant council meeting as required
- reports to Senior Management Team

Network Manager

The Network Manager is responsible for ensuring:

- that the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the School's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that he / she keeps 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 / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator for investigation or action / sanction

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness and understanding of online safety matters and of the current school online safety policy and practices
- they report any suspected misuse or problem to the Online Safety Co-ordinator and Network Manager for investigation / action / sanction
- digital communications with students / pupils (email / voice) should be on a professional level and only carried out using official school systems other than in emergencies
- online safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school online safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / 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

    - They take a responsible attitude towards remote accessing from home
    - That they are fully aware of the guidelines set out within section 33 contained within the Staff Handbook

Designated Safeguarding Lead

should be trained in online safety issues and be aware of the potential for serious child protection 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
- radicalisation and the use of material / online messaging to influence vulnerable children into expressing and acting upon extremist views
- online-bullying
- sexting

IT Steering Group

Members of the *ITSG* assist the *Online Safety Coordinator* with:

- the production / review / monitoring of the school online safety policy / documents.

Pupils

- **are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy.**
- need to develop 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
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- 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 / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

ONLINE SAFETY EDUCATION

Pupils

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum (as part of ICT, PSHE and other lessons) and we continually look for new opportunities to promote online safety.

- Key online safety messages are also reinforced as part of a planned programme of assemblies and tutorial / pastoral activities and informally when opportunities arise
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use. Where free searching of the internet is allowed i.e. using search engines, staff are vigilant in monitoring the content of the websites visited
- Pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff act as good role models in their use of ICT, the internet and mobile devices
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Parents/Carers

Many 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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through

- Letters, newsletters, web site.
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)
- Talks delivered by external Online Safety experts

Staff

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

- A planned programme of formal online safety training is made available to staff in the form of INSET. An audit of the online safety training needs of all staff will be carried out regularly
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas
- The Online Safety Coordinator will receive regular updates through attendance at SWGfL / SSCB / WRAP / other information / training sessions and by reviewing guidance documents released by SWGfL / SSCB / WRAP (Prevent Training) and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training as required to individuals as required

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 policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Manager and will be available to the ITSG.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headmaster or Director of Finance and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by.an end point appliance.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headmaster or Director of Finance
- Any filtering issues should be reported immediately to the IT helpdesk. Any safeguarding concerns should be raised immediately with the respective DSL (KHS / KCT)
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and ITSG (if required). If the request is agreed, this action will be recorded.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential online safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data should be treated with the utmost confidence and in line with the Data Protection Policy.

COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:
When using communication technologies the school considers the following as good practice:

- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any electronic communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and pupils or parents (email, chat) must be professional in tone and content.**

E-MAIL

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private.

Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international.
We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'.

The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. Please see section **33** in the **Staff Handbook** for further staff guidance

All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arranging to meet anyone without specific permission, or accepting virus checking attachments.

Pupils are introduced to e-mail as part of the ICT Scheme of Work.

MANAGING WEB 2.0 TECHNOLOGIES

Web 2.0, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

The school may prevent access to social networking sites to pupils within school, in line with pastoral and academic guidelines.

All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

Our pupils and parents are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

GUIDELINES FOR USE OF COMMUNICATIONS

King's Hall Taunton	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed in line with school policy	Allowed for selected staff	Not allowed	Allowed	Allowed in line with school policy	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		#				#		
Use of mobile phones in lessons		#						#
Use of mobile phones in social time	#					#		
Taking photos on mobile phones or other camera devices		#						#
Use of other mobile devices (tablets, gaming devices	#	#				#		
Use of personal email addresses in school, or on school network	#					#		
Use of school email for personal emails		#				#		
Use of chat rooms / messaging apps		#						#
Use of instant messaging		#				#		
Use of social networking sites		#						#
Use of blogs		#				#		

King's College Taunton	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed in line with school policy	Allowed for selected staff	Not allowed	Allowed	Allowed in line with school policy	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	#					#		
Use of mobile phones in lessons		#					#	
Use of mobile phones in social time	#					#		
Taking photos on mobile phones or other camera devices		#				#		
Use of other mobile devices (tablets, gaming devices		#				#		
Use of personal email addresses in school, or on school network		#				#		
Use of school email for personal emails		#				#		
Use of chat rooms / facilities				#				#
Use of instant messaging		#				#		
Use of social networking sites		#				#		
Use of blogs		#				#		

BREACHES /UNSUITABLE/INAPPROPRIATE 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions - King's Hall Taunton		Acceptable	**Acceptable** in line with School Policy	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**					#
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					#
	adult material that potentially breaches the Obscene Publications Act in the UK					#
	criminally racist material in UK – Radicalisation material					#
	pornography				#	
	promotion of any kind of discrimination – Including Radicalisation				#	
	promotion of racial or religious hatred – Including Radicalisation					#
	threatening behaviour, including promotion of physical violence or mental harm					#
	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				#	
Using school systems to run a private business					#	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					#	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions						#
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					#	
Creating or propagating computer viruses or other harmful files						#
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					#	
On-line gaming (educational)			#			
On-line gaming (non educational)			#			
On-line gambling					#	
On-line shopping / commerce		#				

User Actions - King's Hall Taunton	Acceptable	**Acceptable** in line with School Policy	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
File sharing		#			
Use of social media by pupils				#	
Use of social media by staff		#			
Use of video broadcasting eg Youtube				#	
Use of messaging apps by pupils				#	
Use of messaging apps by staff		#			

User Actions - King's College Taunton		Acceptable	**Acceptable** in line with School Policy	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**					#
	Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003					#
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) contrary to the Criminal Justice and Immigration Act 2008					#
	criminally racist material in UK – Including Radicalisation					#
	pornography				#	
	promotion of any kind of discrimination – Including Radicalisation				#	
	promotion of racial or religious hatred – Including Radicalisation					#
	threatening behaviour, including promotion of physical violence or mental harm					#
	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				#	
Using school systems to run a private business					#	

User Actions - King's College Taunton	Acceptable	**Acceptable** in line with School Policy	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				#	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					#
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				#	
Creating or propagating computer viruses or other harmful files				#	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				#	
On-line gaming (educational)		#			
On-line gaming (non educational)		#			
On-line gambling				#	
On-line shopping / commerce	#				
File sharing				#	
Use of social media by pupils		#			
Use of social media by staff		#			
Use of video broadcasting egYoutube		#			
Use of messaging apps by pupils		#			
Use of messaging apps by staff		#			

BREACHES – RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

A breach or suspected breach of policy by a pupil may result in the temporary or permanent withdrawal of School ICT, hardware, software or services from the offending individual.

Any policy breach by staff will be treated as misconduct and be subject to disciplinary proceedings. In the most serious of cases, it could result in dismissal and may also lead to criminal or civil proceedings.

It is more likely that the 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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. Please see as follows:

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorized use or suspected misuse of ICT must be immediately reported to the school's Online Safety Officer and the Network Manager. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Network Manager.

PUPIL INCIDENTS

King's Hall # - Yes ? - Possible	Refer to form tutor	Refer to Head of ICT / Deputy Head	Refer to Boarding Master / Mistress	Refer to Headmaster	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents	Removal of network / internet access rights	Chance/ Choice/ Consequence	Further sanction e.g .detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		#		#	?		#			#
Unauthorised use of non-educational sites during lessons	#	#						#	#	
Unauthorised use of mobile phone / digital camera / other handheld device	#	#	#					#		#
Unauthorised/ Inappropriate use of social networking / instant messaging / personal email, including out of school if necessary.	#	#				#	#	#		#
Unauthorised downloading or uploading of files	#	#				#		#	#	
Allowing others to access school network by sharing username and passwords	#	#				#		#	#	#
Attempting to access or accessing the school network, using another student's / pupil's account	#	#				#		#	#	#
Attempting to access or accessing the school network, using the account of a member of staff	#	#		#		#	#	#		#
Corrupting or destroying the data of other users	#	#		#			#	#	#	#
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	#	#		#			#		#	#
Continued infringements of the above, following previous warnings or sanctions	#	#	#	#			#	#		#
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	#	#	#	#			#	#		#
Using proxy sites or other means to subvert the school's filtering system	#	#				#		#	#	#
Accidentally accessing offensive or pornographic material and failing to report the incident	#	#							#	
Deliberately accessing or trying to access offensive or pornographic material	#	#	#	#		#	#	#		#
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	#	#							#	

King's College # - Yes ? - Possible	Refer to tutor	Refer to Head of ICT / Deputy Head	Refer to Boarding Master / Mistress	Refer to Headmaster	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents	Removal of network / internet access rights	Warning	Further sanction eg.detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		#	#	#	?		#			#
Unauthorised use of non-educational sites during lessons	#	#						#		
Unauthorised use of mobile phone / digital camera / other handheld device			#					#		#
Unauthorised use of social networking / instant messaging / personal email	#	#				#	#	#		#
Unauthorised downloading or uploading of files	#	#				#		#	#	
Allowing others to access school network by sharing username and passwords		#	#			#		#	#	#
Attempting to access or accessing the school network, using another student's / pupil's account		#	#	?		#		#	#	#
Attempting to access or accessing the school network, using the account of a member of staff		#		#		#	#	#		#
Corrupting or destroying the data of other users		#	#	#		#	#	#	#	#
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		#	#	#	#		#		#	#
Continued infringements of the above, following previous warnings or sanctions	#	#	#	#			#	#		#
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	#	#	#	#			#	#		#
Using proxy sites or other means to subvert the school's filtering system		#	#			#		#	#	#
Accidentally accessing offensive or pornographic material and failing to report the incident	#	#	#						#	
Deliberately accessing or trying to access offensive or pornographic material	#	#	#	#		#	#	#		#
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	#	#							#	

This should be considered in line with the School's Behaviour policy including the Disciplinary sequence.

STAFF INCIDENTS

King's Hall Taunton King's College Taunton # - Yes ? - Possible	Refer to line manager / HR	Refer to Headteacher / DoFin	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	#	#	?	?	#	?
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	#	?				?
Unauthorised downloading or uploading of files	#	?				?
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	#	#				?
Careless use of personal data eg holding or transferring data in an insecure manner	#	#				#
Deliberate actions to breach data protection or network security rules	#	#				#
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	#	#				#
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	#	#				#
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	#	#	?			?
Actions which could compromise the staff member's professional standing	#	#				#
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	#	#				#
Using proxy sites or other means to subvert the school's filtering system	#	?			#	?
Accidentally accessing offensive or pornographic material and failing to report the incident	#	?			#	?
Deliberately accessing or trying to access offensive or pornographic material	#	#	?		#	#
Breaching copyright or licensing regulations	#	?				?
Continued infringements of the above, following previous warnings or sanctions	#	#				#

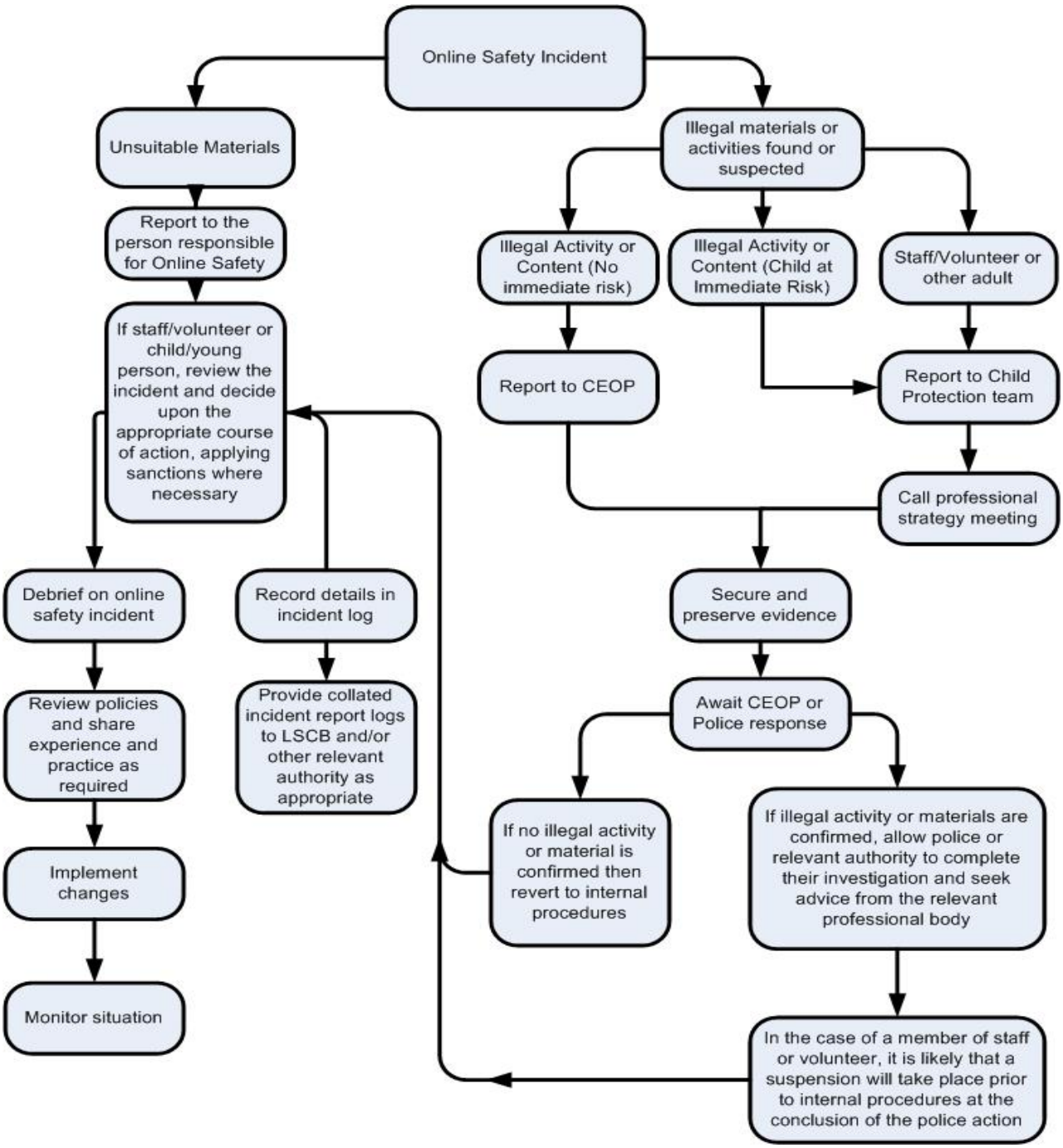
RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material, including material designed to radicalise young people and draw them into terrorism**
- **other criminal conduct, activity or materials**

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 (on the following page) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the 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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures and will be logged as follows:

Online Safety Incident Log

Details of ALL online safety incidents should be recorded by the Online Safety Officer. This incident log will be monitored termly by the Head, Deputy Head Pastoral and Network Manager. Any incidents involving Cyber-bullying should be recorded by the Deputy Head Pastoral.

Table to include:
Date & time
Name of pupil or staff member
Male or Female
Room and computer/ device number
Details of incident (including evidence)
Actions and reasons

SAFE USE OF IMAGES

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Please see the School's Policy on the creation and use of digital and other images of current pupils.

CURRENT LEGISLATION

This online safety document has been written with regard to the following legislation:

Computer Misuse Act 1990
Data Protection Act 2018
Freedom of Information Act 2000
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers Act 2000
Trade Marks Act 1994
Copyright, Designs and Patents Act 1988
Telecommunications Act 1984
Counter Terrorism and Security Act 2015
Criminal Justice & Public Order Act 1994
Racial and Religious Hatred Act 2006
Protection from Harassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 & 1964
Human Rights Act 1998
The Education and Inspections Act 2006
The Education and Inspections Act 2011
The Protection of Freedom Act 2012
Serious Crime Act 2015

And with regard to the following statutory guidance:
Keeping Children Safe in Education 2018

APPENDIX A

KING'S HALL

ICT USER POLICY AND AGREEMENT

I agree that I will:

- Use the school computers to help me research topics for my work.
- Use the school computers to make pieces of work and not use them for gaming or messing around on.
- Use the computers to communicate with members of my family if I don't see them very often i.e. if I am boarding or if my parents go away during term time.
- Keep my personal information and passwords safe and will not give them out to anyone.
- Not use other people's passwords; this includes attempting to log in through another person's account or accessing another person's files (including the Pre-Prep account).
- Only send e-mails that are polite and friendly.
- I will not use language on the internet or in emails that I would not use in front of a teacher.
- Tell a member of staff immediately if I feel uncomfortable or threatened by anything that I see on the internet or receive in an e-mail.

I understand that:

- Using other people's work and claiming that it is my own is a crime.
- That any persistent abuse of the School computer systems will result in my access being suspended or permanently removed.
- I should look after myself and my friends by using the internet in a safe and responsible way.
- The school will deal with cyber-bullying as seriously as any real world bullying incident. I understand that cyber-bullying is when a person or a group of people threaten, tease, embarrass or abuse someone else by using ICT, particularly mobile phones, the internet and related technologies such as social networks.
- The school can monitor the computers at any time and records your 'history'. Using school IT incorrectly and looking, sending or saving of things which are not suitable* is a serious offence.
- This agreement may be amended at any time as seen appropriate by the School.
- Further specific details of policy and sanctions may be requested and can be found in the Online Safety Policy.

Agreement: I have read and agree to these conditions	
Name of Pupil:	Pupil Signature:
Parent / Guardian Signature:	Date:

* The School reserves the right to define unsuitable material

TO BE COMPLETED & RETURNED TO THE SCHOOL OFFICE AS SOON AS POSSIBLE

APPENDIX B

KING'S COLLEGE

ICT ACCEPTABLE USE POLICY – PUPILS

I agree that I will:

- be responsible for all the ICT activity in my area and so will not give my username and password to anybody else.
- not attempt to log on using another person's username and password or access another person's files.
- not attempt to gain unauthorised access to any part of the KCT network that is not available from my personal logon, either via the network or the internet.
- not attempt to use or load programmes, files, tools or shortcuts to gain access to either the C drive of the KCT workstations or any other part of the network.
- immediately report any instance where I have inadvertently gained access to restricted areas to a member of staff.
- only visit websites which are appropriate at the time.
- not visit websites that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of staff.
- not attempt to set-up or use any proxy by-pass software, in order to by-pass the school internet filter.
- Not meet with anyone whom I have made contact with on the internet without discussing this first with my parents/carers/guardians.
- not take information from the internet and pass it off as my own work.
- report any misuse of the internet immediately to a member of staff.
- be responsible in my use of email. I will not include in an email any material that is inappropriate. I will not use offensive or threatening language in my emails or in any other communication on the internet. I understand that any email going out from the school will carry the school address and so represents the school.
- always keep my personal details private.
- only copy pictures or text into my area on the network. I will not download any other type of file, for example software, games, screen savers etc.

In order for King's Schools Taunton to meet legal requirements we now have to make it clear to all students that all activity using any part of the school network is monitored as part of school safeguarding and will be scanned for your own protection. This includes use of personal equipment if linked to the school systems via WiFi or any other means. This policy may be updated or modified at any time should the school deem it necessary and you will be notified the next time you access a school computer. The school reserves the right to administer these rules in a fair and unbiased way, which may result in a student's access to either the internet or the school network being removed or other appropriate sanction being taken. Any questions regarding this policy, please contact the Network Manager.

Agreement: I have read and agree to these conditions	
Pupil Name:	Date:

APPENDIX C

KING'S SCHOOLS TAUNTON
ICT ACCEPTABLE USE POLICY - STAFF

I agree that I will:

- be responsible for all the ICT activity in my area and so will not give my username and password to anybody else.
- not attempt to log on using another person's username and password or access another person's files.
- not attempt to gain unauthorised access to any part of the KCT network that is not available from my personal logon, either via the network or the internet.
- not attempt to use or load programmes, files, tools or shortcuts to gain access to either the C drive of the KCT workstations unless I have access been given permission.
- not attempt to use or load programmes, files, tools or shortcuts to gain access to any other part of the network.
- immediately report any instance where I have inadvertently gained access to restricted areas to a member of the ICT staff.
- only visit websites which are appropriate at the time.
- not visit websites that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of the ICT staff.
- not attempt to set-up or use any proxy by-pass software, in order to by-pass the school internet filter.
- not take information from the internet and pass it off as my own work.
- report any misuse of the internet immediately to a member of the ICT staff.
- be responsible in my use of email. I will not include in an email any material that is inappropriate. I will not use offensive or threatening language in my emails or in any other communication on the internet. I understand that any email going out from the school will carry the school address and so represents the school.
- always keep my personal details private, this includes any data as set out in the data protection policy.
- only copy pictures or text into my area on the network. I will not download any other type of file, for example software, games, screen savers etc.

In order for King's Schools Taunton to meet legal requirements; we now have to make it clear to all staff that all activity using any part of the school network is monitored as part of school safeguarding and will be scanned for your own protection. This includes use of personal equipment if linked to the school systems via WiFi or any other means. This policy may be updated or modified at any time should the school deem it necessary and you will be notified the next time you access a school computer. The school reserves the right to administer these rules in a fair and unbiased way, which may result in staff access to either the internet or the school network being removed or other appropriate sanction being taken. Any questions regarding this policy, please contact the Network Manager.

Agreement: I have read and agree to these conditions	
Staff Name:	Date: