71

King's College
TAUNTON

Online Safety Policy

This policy is applicable to all pupils including those in EYFS

This policy applies to
King's College Prep School and King's College Taunton

Responsibility

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

Review

Last review date: October 2023 (updated post KCSIE 23)

Next review date: October 2024 (in line with updated SWGfL guidance)

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*
- *Data Protection Policy*
- *Policy on Pupils' Use of ICT, Mobile Phones and other Electronic Devices*

INTRODUCTION 2
SCOPE OF THIS POLICY 3
MONITORING 3
ROLES AND RESPONSIBILITIES 5
Head and SMT 5
DSL(this will be the DSL/ DDSL at each school unless otherwise agreed) 5
Network Manager 6
Teaching and Support Staff 6
Designated Safeguarding Lead **Error! Bookmark not defined.**
IT Steering Group 8
Pupils 9
Parents / Carers 9
ONLINE SAFETY EDUCATION 9
Pupils 9
Parents/Carers 10
Staff 10
TECHNICAL – INFRASTRUCTURE / EQUIPMENT, FILTERING AND MONITORING 11
Use of digital and video images 13
COMMUNICATIONS 14
E-MAIL 15
MANAGING WEB 2.0 TECHNOLOGIES **Error! Bookmark not defined.**
GUIDELINES FOR USE OF COMMUNICATIONS 16
BREACHES /UNSUITABLE/INAPPROPRIATE ACTIVITIES 17
BREACHES – RESPONDING TO INCIDENTS OF MISUSE 19
INCIDENT REPORTING 20
PUPIL INCIDENTS 20
King's College Prep 20
King's College 21
STAFF INCIDENTS 23
RESPONDING TO INCIDENTS OF MISUSE 24
Online Safety Incident Log 26
SAFE USE OF IMAGES BY STAFF 26
CURRENT LEGISLATION 26
KING'S COLLEGE PREP 28
IT Pupil Acceptable Use Agreement 28
King's College Prep School policy 28

KING'S COLLEGE 30
ICT ACCEPTABLE USE POLICY – PUPILS 30
KING'S SCHOOLS TAUNTON 31
ICT ACCEPTABLE USE POLICY - STAFF 31
Specific Safeguarding Issues 31

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)
- Youth generated sexual imagery (posting or sending nude or semi-nude images)
- Radicalisation (see child protection and safeguarding policy)
- Online bullying (see anti-bullying policy) and peer on peer abuse
- Access to unsuitable video / internet games
- Online gambling
- 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 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

This online safety policy has been approved by a members of: (delete/add as relevant)

- Headmaster and senior leaders
- Designated Safeguarding Lead
- Staff – including teachers, support staff, technical staff
- Governors

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:	*June 2023*
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

IT Services 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.

IT Services staff may monitor, 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.

Governors

Designated Safeguarding governor is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Educational & pastoral committee which meets termly:

- Termly meetings with the Designated Safeguarding Lead
- regular monitoring of online safety incident logs
- reporting to relevant Governors/Board/Committee/meeting

Head and SMT

- The Head 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 Head / SMT are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. Prevent training is an essential part of this process in both schools
- The Head / 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 Head and 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

Online Safety Coordinator (DSL unless otherwise stated)

Keeping Children Safe in Education states that:
“The designated safeguarding lead should take on the important lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”
They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”
They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online”

The DSLs:-

- hold the lead responsibility for online safety response, within their safeguarding role.
  takes
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online

- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headmaster/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The DSL will 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 and child-on-child abuse (including sexual harassment)
- sharing nudes and semi-nudes/youth generated sexual imagery

Network Manager

is responsible for ensuring that:

- that the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school/college meets required online safety technical requirements and any Local Authority guidance that may apply. 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
- that monitoring software/systems are implemented and updated

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 DSL and Network Manager for investigation / action / sanction

- digital communications with 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
- pupils understand and follow the school online safety and acceptable use policy
- 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 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 the Staff Handbook

IT Services:

The DfE Filtering and Monitoring Standards says:

> "Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."
>
> "Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."
>
> "The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems"

"The IT service provider should work with the senior leadership team and DSL to:
procure systems

- identify risk
- carry out reviews
- carry out checks"

If Members of the ITSG assist the DSL with:
the production / review / monitoring of the school online safety policy / documents.

IT services are responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack

- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).
- monitoring systems are implemented and regularly updated as agreed in school policies

Pupils

the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

- The IT Provider is responsible for ensuring that:
- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).
- monitoring systems are implemented and regularly updated as agreed in school policies

IT Steering Group

Members of the ITSG assist the DSL 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 agreement.
- 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 recognise the consequences and implications 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/ and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile online services and devices in an appropriate way.

The school/college will take every opportunity to help parents and carers understand these issues through :

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/ and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

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 should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- pupils should be 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.
- 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 pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/college.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be 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.
- 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, the school website.
- Reference to the SWGfL Safe website and other similar webpages: saferinternet.org.uk,
- Talks delivered by external Online Safety experts
- High profile events / days e.g. Safer Internet Day

Staff

It is essential that all staff and governors 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 and through Educare courses.

- All new staff receive online safety training as part of their induction programme, and through the staff handbook, ensuring that they fully understand the school online safety policy and Acceptable Use Policies and GDPR issues
- 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 DSL will receive regular updates through attendance at SWGfL / SSCP / other information / training sessions and by reviewing guidance documents released by SWGfL / SSCP / UKCIS and others.
- The DSL will provide advice / guidance / training as required to individuals as required

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in relevant school/college training/information sessions for staff or parents

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/college technical systems will be managed in ways that ensure that the school/college meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school/college technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school/college technical systems and devices.
- All users will be provided with a username and secure password by IT Services who will keep a record of users and their usernames. Users are responsible for the security of their username and password.
- Network Manager is 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 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. There is a clear process in place to deal with requests for filtering changes

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- The school/college has provided differentiated user-level filtering
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place (schools/academies may wish to provide more detail) 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 devices are protected by up to date virus software.
- An agreed protocol is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed protocol is in place regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network.
The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant 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 should be an integral part of the school's online safety education programme.

The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only	-	-	-	*Yes (As appropriate)*	*Yes*	*Yes*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees.

The schools 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 students/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 e.g. on social networking sites.

- 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 e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/academy 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 *students/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 students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

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:

- 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 staff handbook for further 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.

Social Media

Social media and 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.

Sites
The school/college 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
- Regular teaching is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues

GUIDELINES FOR USE OF COMMUNICATIONS

King's College Prep School	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 College Prep School		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, e.g. 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 (e.g. 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 College Prep School

	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 e.g. 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					#	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					#	

User Actions - King's College Taunton	Acceptable	**Acceptable** in line with School Policy	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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 (e.g. 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 e.g. YouTube		#			
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 College Prep # - Yes ? - Possible	Refer to form tutor	Refer to Head of ICT / Deputy Head	Refer to Houseparent	Refer to Head	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 Houseparent	Refer to Head	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents	Removal of network / internet access rights	Warning	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 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 College Prep King’s College Taunton # - Yes ? - Possible	Refer to line manager / HR	Refer to Headteacher / DoF	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 e.g. 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 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	#	#				#

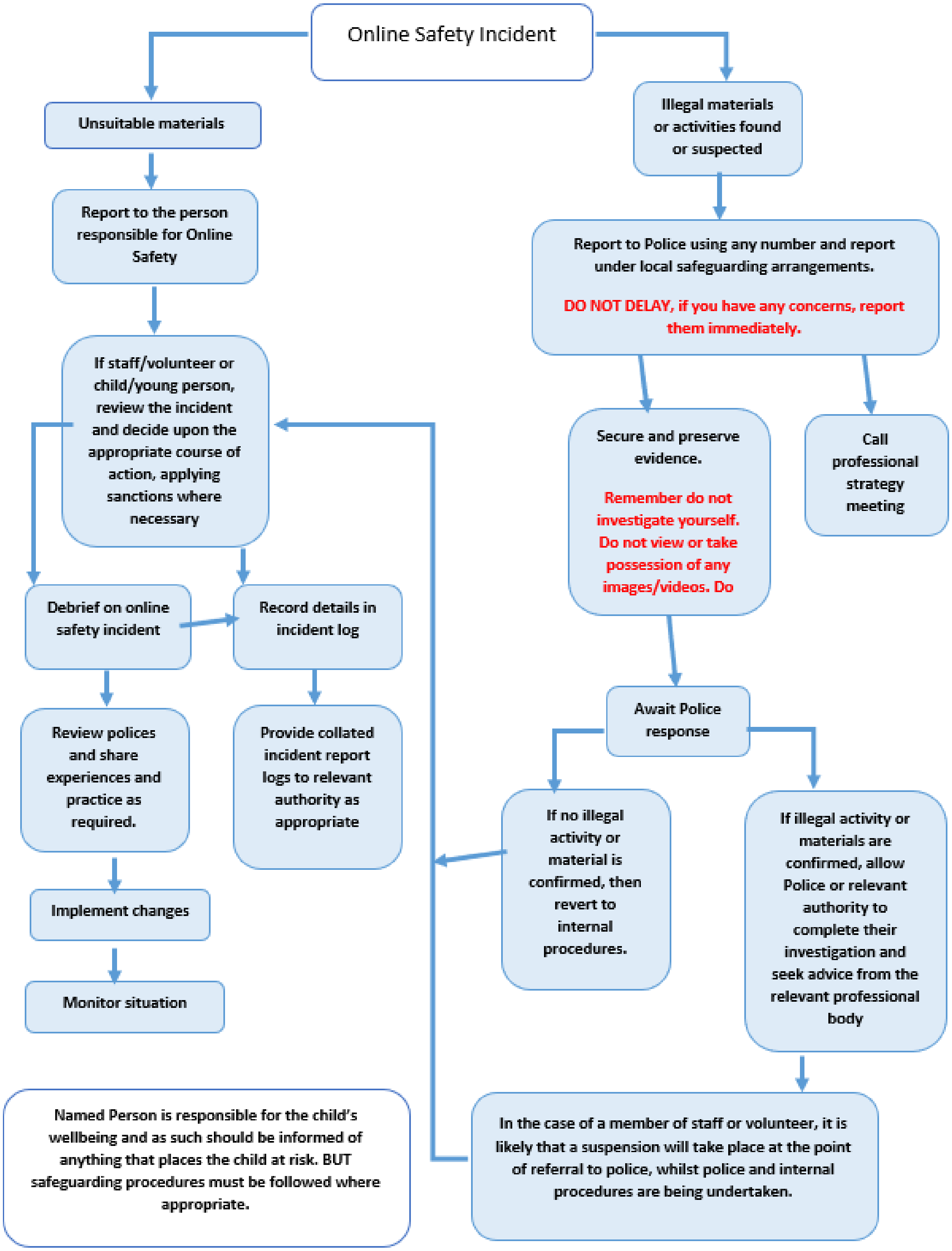
RESPONDING TO INCIDENTS OF MISUSE

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 i.e.

- **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

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await 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 at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

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. Any incidents involving Cyber-bullying should be recorded by the Deputy Head Pastoral.

Table to include:

- **Date & time**
- **Name of pupil or staff member**
- **Room and computer/ device number if known**
- **Details of incident (including evidence)**
- **Actions and reasons**

SAFE USE OF IMAGES BY STAFF

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 Sept 2023

APPENDIX A

KING'S COLLEGE PREP SCHOOL

IT Pupil Acceptable Use Agreement

King's College Prep School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will not communicate on-line to other adults or young persons who I do not know, I will not arrange to meet them unless with a responsible adult and my parents/guardians and staff at school are aware.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite, respectful and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not intentionally open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use approved social media sites with permission and at the times that are allowed. This will only be for academic reasons authorised by a member of staff.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

I/We confirm that I/we have read the above with my/our child and that he/she understands and agrees to follow the rules included in the acceptable use agreement when:

- Using the school systems and devices (both in and out of school)
- Using personal devices in the school (when allowed) e.g. mobile phones, gaming devices, USB devices, cameras etc.
- Using personal equipment out of school in a way that is related to being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

This form is completed via the School Portal.

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.
This form is completed electronically.

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 Wi-Fi 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:

APPENDIX D

SPECIFIC SAFEGUARDING ISSUES

Child on Child Abuse

All members of staff are made aware that children can abuse other children (often referred to as child-on-child abuse). Children are encouraged to talk to members of staff if they feel they are the victim or perpetrator, or if they are aware of child-on-child abuse. This abuse may include:

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's anti-bullying policy. The school will follow procedures in place to support anyone in the school community affected by cyberbullying.

- Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, contacting Childline via the website, App and phone number 0800 1111, POSH helpline 0344 381 4772.

- Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.

- All incidents of online bullying reported to the school will be recorded and action taken by the school.

- The school will follow procedures to investigate incidents or allegations of cyberbullying.

- The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

- Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.

- Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy or AUP and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content

- internet access being suspended at the school for a period of time.

- the parent and carers of pupils being informed

- the police being contacted if a criminal offence is suspected

Sexting / Sharing nudes

The school will follow UKCIS advice on how to respond to any incident of sexting. We will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

Sexual Harassment, including Upskirting

All staff are made aware that sexual harassment can occur between two children of any age and gender and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including on social media
- sexual exploitation; coercion and threats
- upskirting

All staff are made aware of what upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the Designated Safeguarding Lead (DSL). The Designated Safeguarding Lead (DSL) will record the incident(s) and the actions taken in line with statutory guidance and advice from Somerset Local Authority and/or the police as necessary.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.