E-Safety Policy

All Kings' policies will be ratified by the Board of Directors and signed by the Chairperson. Each policy will be co-signed by the Principal of each school. Review dates will be similar for each school.

Coordinator	Nominated Director	Chair of Board of Directors
PRINCIPAL	**DIRECTOR OF COLLEGE SERVICES**	**NIGEL PAMPLIN**

We have a duty to provide students with Internet access as part of their learning experience across all curricular areas. The use of the Internet is an invaluable tool in the development of lifelong learning skills. We believe that used correctly Internet access will not only raise standards, but it will support teacher's professional work and it will enhance the school's management information and business administration systems.

We acknowledge that the increased number of mobile communication technologies in and out of school brings with it the need to ensure that learners are safe. We also recognize that the school has limited control of these technologies outside the school environment. We need to teach students how to evaluate Internet information, the information they are disclosing, and to take care of their own safety and security in school and beyond.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremist groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views. (See also, Kings Preventing Extremism and Radicalisation Policy)

Effective E-Safety, which encompasses Internet technologies and electronic communications, will educate students, staff and host carers about the benefits and risks of using technology and provide safeguards and awareness to enable them to control their online experience.

We believe this policy relates to the following legislation (click on the link below to access information):

- Children Act 1989
- The Education (Independent School Standards) (England) Regulations 2014
- Equality Act 2010
- The Computer Misuse Act 1990
- Obscene Publications Act 1959
- Police Act 1997
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Children and Young Persons Act 2008
- Protection of Freedoms Act 2012

- Counter Terrorism and Security Act 2015

The following documentation and online guidance is also related to this policy (click on the link below to access information):

- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- Childnet International - http://www.childnet.com/teachers-and-professionals
- 360 Safe - http://www.360safe.org.uk/Home
- South West Grid for Learning - http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources
- Wise Kids - http://wisekids.org.uk/wk/
- E-safety - Developing whole-school policies to support effective practice (Wise Kids)
- Advice for parents and carers on cyberbullying (DfE)
- Cyberbullying: advice for headteachers and school staff (DfE)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

Aims

- To make education, rather than software, the most effective tool in maintaining E-Safety;
- To ensure that all Internet users are aware of the risks and the benefits of using the Internet and other technologies to find and share information;
- To provide guidance that students can use to protect themselves outside the classroom;
- To allow reasonable access to the valuable range of educational resources on offer online;
- To ensure that the same values and knowledge are shared by students, staff, and host carers.
- To work with other organisations to share good practice in order to improve this policy.

Procedure

Role of the Board of Directors	The Board: ▪ has delegated to the Principal the appointment of a member of staff as E-safety Coordinator, to be responsible for E-Safety; ▪ has delegated powers and responsibilities to the Principal to ensure all school personnel are aware of and comply with this policy; ▪ has responsibility for ensuring funding is in place to support this policy; ▪ has responsibility for ensuring this policy is made available to parents; ▪ has responsibility for the effective implementation, monitoring and evaluation of this policy ▪ has nominated the Director of College Services to visit the school regularly, to liaise with the Principal and E-Safety Coordinator and to report back to the Board of Directors; ▪ will annually review all safeguarding policies and procedures; ▪ has responsibility for the effective implementation, monitoring and evaluation of this policy
Role of the Principal	The Principal will: ▪ ensure the implementation of this policy; ▪ ensure all school personnel, students, host carers and parents are aware of and comply with this policy; ▪ nominate a member of staff as the E-Safety Coordinator; ▪ work with the advice of other organisations and the E-Safety Coordinator to create a safe ICT learning environment both at school and in residential accommodation by having in place: - an effective range of technological tools - clear roles and responsibilities

	- safe procedures - education - clear boundaries and parameters for the use of technology, personal devices and online resources in class and school; - a comprehensive policy for students, staff, host carers and parents; ▪ authorised training for the E-Safety Coordinator in order to understand E-Safety issues and procedures; ▪ along with the E-Safety Coordinator and IT Manager receive and respond to any reports of internet/digital media misuse (see appendix C); ▪ monitor the effectiveness of this policy; ▪ meet annually with the Director of College Services and E-Safety Coordinator to review the effectiveness of the policy ▪ undertake student consultation to obtain feedback on this policy
Role of the Director of College Services	The Director of College Services will: • regularly visit the school's Principal and E-Safety Coordinator to ensure the policy is implemented effectively; • report back to the Board of Directors
Role of E-Safety Coordinator	The E-Safety Coordinator will: ▪ work closely with the IT Manager and Principal; ▪ coordinate regular meetings of the E-Safety Group to share developments, review policy and ensure school-wide participation with this policy; ▪ ensure the E-Safety Group are made aware of a list of inappropriate access attempts, in order to review filtering provision; ▪ along with the Principal and IT Manager receive and respond to any reports of internet/digital media misuse (see appendix C); ▪ receive regular training in order to understand current E-Safety issues and procedures; ▪ annually review the school's practices and procedures with an aim to improving E-Safety, ▪ work with the advice of other organisations such as *Childnet*, *360 Degree Safe* and *The South West Grid for Learning* to create a safe ICT learning environment; ▪ lead the development of this policy and best practice throughout the school and residential accommodation for both staff, host carers and students; ▪ provide, or facilitate the provision of, education and guidance to students on good E-Safety practice through workshops or visiting speakers; ▪ provide education, guidance and support to staff and host carers on good practice in E-Safety through guidance information, workshops or visiting speakers; ▪ provide information to parents on the E-Safety work being done in school, where necessary; ▪ ensure that students sign the Student Acceptable Use Agreement (appendix B) at induction and are made aware of any updates, as and when they arise; ▪ ensure that all Internet users are kept up-to-date with new dangers, guidance and procedures; ▪ provide training for staff on induction and when the need arises, ensuring they are also aware of the Staff Acceptable Use Agreement (see HR Policy Manual); ▪ ensure host carers are aware of basic E-Safety principals (appendix A), to allow them to promote E-Safety and support students in their care; ▪ keep up-to-date with new developments and resources; ▪ work with school IT Teams in safeguarding student and staff access to some material through education; ▪ review and monitor the policy; ▪ annually review the policy and practices with the Principal and Director of College Services
Role of the IT Manager	The IT Manager will: ▪ work closely with the E-Safety Coordinator and Principal; ▪ work with the Principal and E-Safety Coordinator to ensure adequate

	measures are in place to restrict access in both the school and any residential accommodation to inappropriate online content such as filtering; ▪ along with the Principal and E-Safety Coordinator receive and respond to any reports of internet/digital media misuse (see appendix C); ▪ along with the E-Safety Coordinator, ensure that the Acceptable Use Agreements are understood and followed by all in school; ▪ ensure that an effective range of technological tools exist that promote E-Safety while allowing reasonable access to online resources; ▪ ensure that new programs will be installed onto the network or stand-alone machines by school IT technicians only; ▪ use appropriate Anti-virus software; ▪ set parameters for the use of personal data storage devices in school, so as to ensure sensitive information cannot be obtained inappropriately and external viruses cannot be downloaded onto school computers; ▪ ensure that everyone in school is aware that under *the Computer Misuse Act 1990* the use of computer systems without permission or for inappropriate use could constitute a criminal offence.
Role of the E-Safety Group	The E-Safety Group will be made up of the following: ▪ Principal ▪ E-Safety Coordinator ▪ IT Manager ▪ Welfare Officer ▪ Senior Academic Department Member (i.e. DoS/ADoS) ▪ Senior EFL Department Member (i.e. DoS/AdoS) ▪ ICT teaching staff Members of the E-safety Group will assist the E-Safety Coordinator (or other relevant person, as above) with: ▪ disseminating e-safety information to staff, host carers and students; ▪ the review and monitoring of the school e-safety policy; ▪ the review and monitoring of the school and residential accommodation filtering system and requests for filtering changes; ▪ mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression; ▪ monitoring network / internet / incident logs; ▪ consulting stakeholders – including parents / carers and the students about the e-safety provision;
Role of School Personnel	School personnel will: ▪ comply with all aspects of this policy; ▪ undertake appropriate training; ▪ accept the terms of the Staff Acceptable Use Agreement before using any Internet resource in school; ▪ are responsible for promoting and supporting safe behaviours with students and E-Safety procedures; ▪ will ensure that the use of Internet-derived materials complies with Copyright Law
Role of Host Carers	Host carers have a responsibility to assist the school in E-Safety provision. They should be made aware of E-Safety issues, reporting concerns and given guidance on making their home networks safe and secure.
Internet Filtering and Use	We have a contract with a reputed and national Internet provider to manage a secure and filtered Internet service which enables us to safely access and use the Internet and all email. The Internet filtering service will be annually reviewed. Access to the Internet is designed to protect pupils and school personnel by blocking the following content: ▪ adult content containing sexually explicit images ▪ violent content containing graphically violent images ▪ hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds

	▪ illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs ▪ criminal content relating to the promotion of criminal and other activities ▪ gambling content relating to the use of online gambling websites All users access the Internet in accordance with the School's Acceptable Internet Use & Agreement and will inform the E-Safety Coordinator and IT Manager if at any time they find they have accessed inappropriate Internet sites. When inappropriate material has been accessed the Internet Service Provider will be contacted and if necessary the Police.
Role of Students	Students will be aware of this policy and will be asked to: ▪ accept the terms of the Student Acceptable Use Agreement before using any Internet resource in school or residential accommodation; ▪ be critically aware of the materials they read; ▪ validate information before accepting its accuracy; ▪ acknowledge the source of information used; ▪ use the Internet for research; ▪ respect copyright when using Internet material in their own work; ▪ be aware of the risks of using geo-location tools; ▪ be aware of the risks of sharing personal information online; ▪ be aware of the information they share about others; ▪ be aware of the effect of their 'digital footprint' on university and job applications; ▪ only use approved e-mail accounts; ▪ never take part in 'trolling' or any form of online abuse; ▪ report receiving any offensive e-mails; ▪ not divulge their or others personal details; ▪ not arrange to meet anyone via e-mail; ▪ seek authorisation to send a formal e-mail to an external organization; ▪ not take part in sending spam
Student Consultation	We wish to consult our students and to hear their views and opinions as we acknowledge and support Article 12 of the United Nations Convention on the Rights of the Child that children should be encouraged to form and to express their views. Student consultation is integral to our process of regular self-evaluation and continuous improvement and will take place in a variety of ways. The methods will include: • A Student Forum/Council (which will meet regularly and also be consulted by the Principal) • An appointment system and means of contact with the Principal and key staff members • Operating an 'open door' policy in school whenever possible • Student Questionnaires (on a variety of matters relating to the school and/or and social issues) • Open Class discussion (on a variety of matters relating to the school and/or and social issues) • Suggestion Box (allowing anonymity if desired) Every effort is made to provide a variety and range of consultation methods to all students. Every student who attends a course at Kings will be encouraged and given the opportunity to provide feedback on every aspect of school life during their stay with us. A separate policy exists for student consultation which explains these processes in more detail.

Internet Use	The school Internet access will: ▪ be designed for student use; ▪ include filtering appropriate to the age of students; ▪ be reviewed and improved by the IT Team and the E-Safety Coordinator
Authorising Internet Access	▪ Before using any school ICT resource, all students and staff must read and sign the 'Acceptable ICT Use Agreement' (appendix B and HR Policy Manual) All students and school personnel who are issued with a personal ID and logon, should not divulge the details to anyone.
School Website	Contact details on the website will be: ▪ the school address ▪ e-mail address ▪ telephone number The school website will not publish: ▪ staff or students' contact details
Complaints: School Personnel	The Principal will deal with all complaints of Internet misuse by school personnel (please refer to appendix D, the *Kings Complaints Policy*, and *Staff Grievance* section of the HR Manual)
Complaints: School Students	The Principal will deal with all complaints of Internet misuse by school students (please refer to appendix D and *Kings Behaviour and Discipline Policy*). Parents will be informed if their child has misused the Internet.
Role of Parents and their Representatives (if they are the fee-payers)	Parents and their Representatives will: ▪ be aware of and comply with this policy; ▪ be asked to support the E-Safety policy
Raising Awareness of the Policy	We will raise awareness of this policy using: ▪ the school website ▪ the Staff Handbook ▪ the HR Policy Manual ▪ the Student Handbook ▪ the Teacher Handbook ▪ student lessons ▪ staff training ▪ information displays in the school
Associated Policies and Publications	This policy has been written with reference to and in accordance with the following policies and publications: • Kings Safeguarding & Child Protection Policy • Kings Behaviour and Discipline Policy • Kings Anti-Bullying Policy • Kings Preventing Extremism and Radicalisation Policy • Kings Student Handbook • Kings Staff Handbook • Kings HR Manual The published Aims and Ethos of the School
Monitoring the Effectiveness of the Policy	The effectiveness of this policy will be reviewed annually, or when the need arises, and the necessary recommendations for improvement will be made to the Board of Directors.

Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

This policy affects or is likely to affect the following members of the school community (✓)	Pupils	School Personnel	Parents/ carers	Directors	School Visitors	Wider School Community
	✓	✓	✓		✓	✓

Question	**Protected Characteristics**								**Conclusion**	
Does or could this policy have a negative impact on any of the following?	Age	Disability	Gender	Gender identity	Pregnancy or maternity	Race	Religion or belief	Sexual orientation	Undertake a full EIA if the answer is 'yes' or 'not sure'	
YES									**Yes**	**No**
NO	✓	✓	✓	✓	✓	✓	✓	✓		✓
UNSURE										
Does or could this policy help promote equality for any of the following?	Age	Disability	Gender	Gender identity	Pregnancy or maternity	Race	Religion or belief	Sexual orientation	Undertake a full EIA if the answer is 'no' or 'not sure'	
YES	✓	✓	✓	✓	✓	✓	✓	✓	**Yes**	**No**
NO										✓
UNSURE										

Conclusion	We have come to the conclusion that after undertaking an initial equality impact assessment that a full assessment is not required.

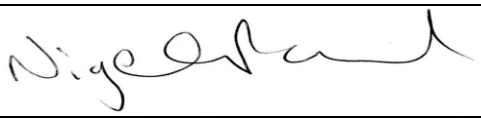
Annual Policy Review Sheet – Appendix 1:

Review Date	Primary Reviewer Name (Policy Coordinator)

This Appendix A should be completed **annually** by the Policy Coordinator and Principal with specific details of each individual Kings college.

Date of Last Review:	
Date of Next Review:	
Is this policy being implemented fully, with all outlined procedures followed as prescribed?	YES/NO
The E-Safety Group members in this School are:	Insert names:
When did the E-Safety Group last meet?	XX/XX/XXXX
Are sufficient measures are in place to restrict access to inappropriate online content, such as filtering?	YES/NO
Have above measures been reviewed in the past 12 months – to take into account new developments and any reported incidents in school?	YES/NO
Have any incidents of ICT misuse been reported in the last 12 months?	Number of Incidents: X
Is E-Safety Education in place for all compulsory school age students?	YES/NO
Are all students and staff asked to sign the *Acceptable ICT Use Agreements* (appendix B and HR Policy Manual)?	YES/NO
If this policy is not being implemented fully, as prescribed, please outline what you have put in place instead and the reasons behind the change...	
How are staff made aware of this policy?	
Does this policy require any specific/specialised training for staff, if yes please specify what it is and whether it has been done?	

Monitoring the Effectiveness of the Policy **The information in this policy and appendix will be reviewed annually by the Principal, or when the need arises, and the necessary recommendations for improvement will be made by the Principal to the Board of Directors.** **Please comment on the overall effectiveness of this policy – giving any suggestions or recommendations for improvement…**

Coordinator:		**Date:**	
Principal:		**Date:**	
Chair of Board of Directors:		**Date:**	01/01/2015
Name of School:			
Next Review Date:			

Appendix A – E-Safety Guidance and Advice

An overview of the risks of ICT use

Taken from E-safety - Developing whole-school policies to support effective practice (Wise Kids/ BECTA)

ICT can offer many positive educational and social benefits to young people, but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. Some of the issues and risks are summarised below.

While many of the issues outlined in this section relate, primarily, to ICT use outside school, it is inevitable that some of the issues, when initiated outside school, will be bought back in and need to be dealt with accordingly by the school. For example, bullying via chat or text messages will impact upon relationships within school; obsessive use of the internet may impact upon the quality of schoolwork; and changes in the personality and general wellbeing of a pupil may indicate that they are involved in inappropriate or illegal behaviours online.

Schools will have technologies in place to restrict inappropriate access, but it must be borne in mind that children will bring an increasingly sophisticated range of handheld devices into school giving them separate access to potentially unsuitable materials. Hence schools' acceptable use policies will also need to consider pupils' own equipment. Schools therefore have a major responsibility to educate their pupils; 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. Young people who have been using the internet excessively, or engaging in risky or illegal behaviours online, may benefit from professional support or counselling to redress the balance of their online and offline life. The school may play a key role in recognising this need, and engaging appropriate help.

Copyright infringement

Copyright law applies on the internet, but is ignored by many young people who download and swap music files, cut and paste homework assignments from others' work, or even purchase whole assignments from online cheat sites without realising the implications and consequences.

Obsessive use of the internet and ICT

There is the potential for children and young people to become obsessed with the internet and related technologies. Factors such as spending a significant amount of time online, deterioration of the quality of school work, diminished sleep time, or negative impacts upon family relationships, may all be indicators that the internet is taking too high a priority in a young person's life.

Exposure to inappropriate materials

There is a risk that when using the internet, email or chat services, young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature, encourages activities that are dangerous or illegal, or is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexist views are able to spread their distorted view of the world.

In the case of pornography, there is no doubt that the internet plays host to a large amount of legal and illegal material.

Curiosity about pornography is a normal part of sexual development, but young people may be shocked by some of the material online. It is not known what the long-term effects of exposure to such images may be.

Inappropriate or illegal behaviour

Young people may get involved in inappropriate, antisocial or illegal behaviour while using new technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious. Online bullying is an unfortunate aspect of the use of new technologies, perceived as providing an anonymous method by which bullies can torment their victims at any time of day or night. While a young person may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing. Some children and young people may become involved in much more serious activities. Possible risks include involvement in identity theft or participation

in hate or cult websites, or the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites for the sale of weapons, hacking sites, and sites providing recipes for drug or bomb making are also of great concern.
Young people may also become involved in the viewing, possession, making and distribution of indecent and/or child pornographic images. Any concern relating to criminally obscene or criminally racist content can be reported to the Internet Watch Foundation or the police.

Physical danger and sexual abuse

The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies. A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. Paedophiles will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop over days or weeks, or even months or years, as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact such as text messaging as a prelude to meeting in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.
The Sexual Offences Act 2003, which came into force in May 2004, includes a grooming offence specifically introduced to combat this abuse of the internet and young people.
There is also a risk that while online a young person might provide information that can personally identify them or others, or arrange to meet people they have met online, so posing a risk to their safety or that of their family or friends.

Inappropriate or illegal behaviour by school staff

Unfortunately, school staff have also been found to have been involved in inappropriate or illegal behaviour relating to ICT use. This may include viewing or circulating inappropriate material via email, or much more serious activities such as viewing, possessing, making or distributing indecent and/or child pornographic images. Schools also have a responsibility, therefore, to educate staff as to acceptable behaviours online, and to monitor school networks for evidence of inappropriate activity. Inappropriate activity by a staff member may result in a disciplinary response by the school or authorities. If illegal behaviour by a staff member is suspected, the school has a duty to consult with the police at the earliest opportunity, preserving any potential evidence.

E-Safety Hot Topics

Taken from Childnet International - http://www.childnet.com/parents-and-carers/hot-topics

Cyberbullying

Cyberbullying is when someone uses technology, such as the internet or a mobile device to bully others.

Being a victim of cyberbullying can be very distressing for a young person and occasionally they don't know who is bullying them. Cyberbullying includes things such as sending nasty text messages or emails, or setting up a hate group on a social networking site. The bullying may also happen 24/7 and the victim is often targeted even when they are in the comfort of their own home. Images and text messages can be circulated very quickly and widely on the internet which can make it difficult to combat cyberbullying.

Sexting

What is sexting?
Sexting [verb] = sending sexually explicit content
The term 'sexting' describes the use of technology to share intimate images of yourself. It's a word-mix of sex and texting. The content can vary, from text messages to images of partial nudity to sexual images or video.
Sexting often happens when a young person's judgment has been clouded, e.g by pressure from someone else, or from the use of alcohol or drugs. This content is usually created to be sent to a partner, but can be between groups and can use a range of mobile devices, technologies and online spaces. Photos and videos are often created via webcam or Smartphone camera, and are shared on social networking sites such as Facebook, Twitter, Tumblr, Flickr and Snapchat, messaging services such as IM or BBM, and video sites such as YouTube.

Is it legal? Sexting and the Law

If a young person under the age of 18 engages in sexting by creating an explicit photo or video of themselves, they could be held responsible for creating an image of child abuse. Sending this content on to another person is the distribution of an image of child abuse. By receiving content of this kind from another young person, they could be held responsible for possessing an image of child abuse.

The Association of Chief Police Officers of England, Wales and Northern Ireland have stated that young people engaging in sexting should be treated as victims in the first instance and not face prosecution as first time offenders, but the situation will be investigated to ensure the young people involved are not at risk. The police's priority is those who profit from sexual images. Repeat offenders and more extreme cases are reviewed differently, still with a focus on avoiding prosecution unless absolutely necessary.

If someone is pressurising your child to send them a sexting image, inform the police. Not only is it illegal, but it may prevent them from doing it to someone else too.

Social networking

Social networking sites such as Facebook and Twitter are very popular with young people, even those who are of primary age. These types of sites allow young people to be incredibly creative online, keep in touch with their friends as well as sharing photos and videos.

Many sites have a minimum user age of 13, although some interactive sites are designed specifically for younger children.

Young people need to protect their online reputation

Young people use social networking sites for many different purposes; to communicate with their friends, to share content and to find out new information. You need to remind your child that they need to be careful about what they're posting online. Children can sometimes believe that social networking sites are a private space for them and it can be difficult for them to realise that what they're posting online may be publicly visible and can be spread very quickly to a large audience.

The blur between public and private expression can potentially put a child at risk in two main ways:

Content

Content which is uploaded online can be copied, altered and reposted by anyone and it is very difficult to 'take back' what may be later regretted. Children who create or post inappropriate, offensive or even illegal content on their own or others' web pages could get them into trouble with their school, friends and even the police, depending on the nature of the material.

Contact

Young people need to be aware of how much personal information they upload onto these sites. If a user of a social networking site doesn't protect their information by enabling the correct privacy settings, they could be exposing their information to adults with a sexual interest in children. Posting or chatting about personal details might enable someone to identify and contact your child online or in person. Sharing personal information may also increase the risk of cyberbullying.

Downloading

There are many great ways of accessing and downloading music, film, TV and video safely online and it is important that children and young people understand how to download content legally.

1. Music, film and TV on the internet - what you should know:

Copyright law applies to downloading, sharing and streaming just as in the world of physical CDs and DVDs. If you make music, film or TV content available to others on a file-sharing network, download from an illegal site, or sell copies without the permission of those who own the copyright, then you are breaking the law and could face serious penalties.

2. Staying tuned in while staying legal:

There is a wide choice of legal sites where you can download or "stream" (transmit over the internet) music, film or TV content. Some are stores where you can buy downloaded tracks, albums, TV shows, videos or films to play on a computer, or a portable device or on a music player. Others charge a monthly subscription fee and let you stream from an internet-connected device at any time. Some services provide entertainment for free, supported by advertising.

3. What you can and can't do with music, film and TV online:

It is illegal to upload or download copyrighted files without permission from the person who owns the

rights. File sharing services can in theory be used legally, but in practice nearly all the content on them is illegal. The only safe way to use them legally is to be sure you are sharing materials that are not protected by someone else's copyright.

4. Staying safe and responsible:
Illegal file-sharing programmes and websites pose greater risks to your computer or mobile phone than legitimate sites. Users often unwittingly download viruses or spyware and can inadvertently share personal computer files and information. Some files are purposely misnamed on file-sharing and peer-to-peer networks to trick people into downloading them.

Gaming

Online gaming is hugely popular with children and young people. Recent research shows that gaming is one of the top activities enjoyed by 9-16 year olds online, with gaming more popular than social networking.
From sport related games, to mission based games and quests inspiring users to complete challenges, interactive games cater for a wide range of interests, and can enable users to link up and play together. Games can provide a fun and social form of entertainment often encouraging teamwork and cooperation when played with others.
Just like offline games, they can have educational benefits, and be used, for example, to develop skills and understanding. Traditionally, games could be bought from shops, often in the form of a disk for use on a PC or console. Now, games can also be downloaded online. Games are played on many platforms, with those bought in shops often having an online component to them. Internet connectivity in a game adds a new opportunity for gamers as it allows players to find and play against, or with, other players from around the world (in a multi-player game).
There are many ways for users to play games online. This includes free games found on the internet, games on mobile phones and handheld consoles, as well as downloadable and boxed games on PCs and consoles such as the PlayStation, Nintendo Wii or Xbox.

Online grooming

The internet can be a fantastic place for children and young people to connect with their friends, discover new things and be creative. However, 'friends' made online may not be who they say they are. This is a difficult concept for children to understand.
Online grooming is the process by which an adult with an inappropriate sexual interest in children will approach a child online, with the intention of fostering a relationship with that child, to be able to meet them in person and intentionally cause harm. For more information and age appropriate resources for children relating to online grooming, visit **Thinkuknow**.

Online Dating

Online dating has become very popular over recent years and many young people see it as a legitimate way of meeting people. Apps or websites such as Tinder, Zoosk, Match.com and Plenty of Fish give users access to personal information and photographs in much the same way as Facebook or other social networking sites, but with the added risk of users purposefully making this information available to people they do not know and have never met. Though online dating can be very positive, it is important that users know the risks. Most dating websites or apps have an age limit of 18 or over, however, this is unlikely be verified, so it is easy enough for under 18s to sign up. Anyone using online dating sites should be aware that: the people they are talking to may not be who they say they are or may have misrepresented themselves; photographs can be viewed by anyone using the site and once uploaded are in the public domain; details such as address, phone number or work location should not be openly disclosed; users should be extremely cautious about revealing personal or intimate information. If arranging to meet someone from an online dating site, every care should be taken to stay safe, i.e. tell someone where you are going and arrange to call or text regularly throughout the date, go somewhere public and close to home etc.

Premium Rate Content

Buying content for your phone - apps
Mobile phone downloads and apps are very popular among young people and are easily available from websites and online services such as Apple's App Store and Google Play.
Often when one emerges it can quickly becomes '*the* thing' to have and talk about in the playground. A lot of popular apps are free to download, but this does not mean they won't charge you later on – many games are free up to a point, before then asking for a payment in order to continue onto the next level or to access additional features.
When involved in the game and eager to progress further, it's easy for a child to just click to 'pay and continue' despite any messages asking them to confirm this, and for them not to consider the cost. The charge of 'playing on' may be less than a pound per time, but this can mount up very easily. Some transactions can cost considerably more.

Buying content for your phone – premium rate services
There are a number of services available that allow users to sign up via their mobile phone number to download ringtones, music, video and other content. These are very popular amongst young people, but it is important to be aware that by signing up for the service, they may have signed up for a subscription. Rather than just paying one charge for access to new content, they could be charged over and over again without realising.

Appendix B – Student Acceptable ICT Use Agreement

Academic Student - Acceptable ICT Use Agreement

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

For my own personal safety:

- I understand that Kings will monitor my use of computer 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 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, financial details etc).
- I understand that making 'friends' with people online can be dangerous if I do not know them in person – as they may not be who they say they are.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and make sure a member of Kings staff or my homestay carer knows where I am, who I am meeting and what I am doing.
- 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 Kings' 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 Kings' systems or devices for on-line gaming, on-line gambling, file sharing, or video broadcasting (eg 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 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 use social networking sites or any other form of technology to bully, harass or be unkind to others.
- I will not take or distribute images of anyone without their permission.

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

- 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 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 social media sites out-side lesson times and not on classroom computers, unless I have permission.

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

- I will not plagiarise the work of others – copy, borrow or use the ideas or work of other people or organisations and present them as my own.
- I will ensure that I have permission to use the original work of others in my own work and use appropriate referencing to show where it has come from.
- 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.

When using my own personal devices (mobile phone, tablet/iPad, laptop computer etc):

- I understand that, if I use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand that I may only use my own devices in class time if I have permission from my teacher.
- I understand that school staff may ask me to switch off my personal devices during class time and other times during the school day and I must do this if asked to.
- If I do not follow the rules set out by this agreement I may be asked to leave my personal devices at home or may have them confiscated until the end of the school day.
- If I bring my own personal devices to school I do so at my own risk and understand that it is my responsibility to keep them safe.
- I will not use or borrow personal devices from others unless I have their permission to do so.

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

- I understand that Kings 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 cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable ICT Use Agreement, I will be subject to disciplinary action. This may 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.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access may not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email/website/Facebook page etc.

Name of Student	
Course	
Signed	
Date	

EFL Student - Acceptable ICT Use Agreement

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

I will stay safe online:

- I understand that Kings will monitor my use of computer systems, devices and digital communications.
- I will not give other people my usernames or passwords.
- I will not share personal information about myself or others when on-line.
- I will be careful when talking to people online that I do not know.
- I will immediately report any unpleasant or inappropriate material or messages.

I will respect Kings ICT equipment:

- I will not make large downloads or uploads; or upload, download or access anything which is illegal or inappropriate.
- I will not use Kings' systems or devices for on-line gaming, on-line gambling, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I will report any damage or faults involving equipment or software.
- I will not 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 social media sites out-side lesson times and not on classroom computers, unless I have permission.

I will respect other users of ICT:

- I will not access, copy, remove or change any other user's files or work.
- I will be polite and respectful when communicating with others.
- I will not use technology to bully, harass or be unkind to others.
- I will not take or distribute images of anyone without their permission.

I will not use other people's work and say it is my own (plagiarism).

When using my own personal devices (mobile phone, tablet/iPad, laptop computer etc):

- I will follow the rules in this agreement when I am using my own devices.
- I understand that school staff may ask me to switch off my personal devices during class time.
- If I do not follow the rules set out by this agreement I may be asked to leave my personal devices at home.
- If I bring my own personal devices to school I do so at my own risk and understand that it is my responsibility to keep them safe.
- I will not use or borrow personal devices from others unless I have their permission to do so.

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

- I understand that Kings 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 cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable ICT Use Agreement, I will be subject to disciplinary action.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access may not be granted to school ICT systems.

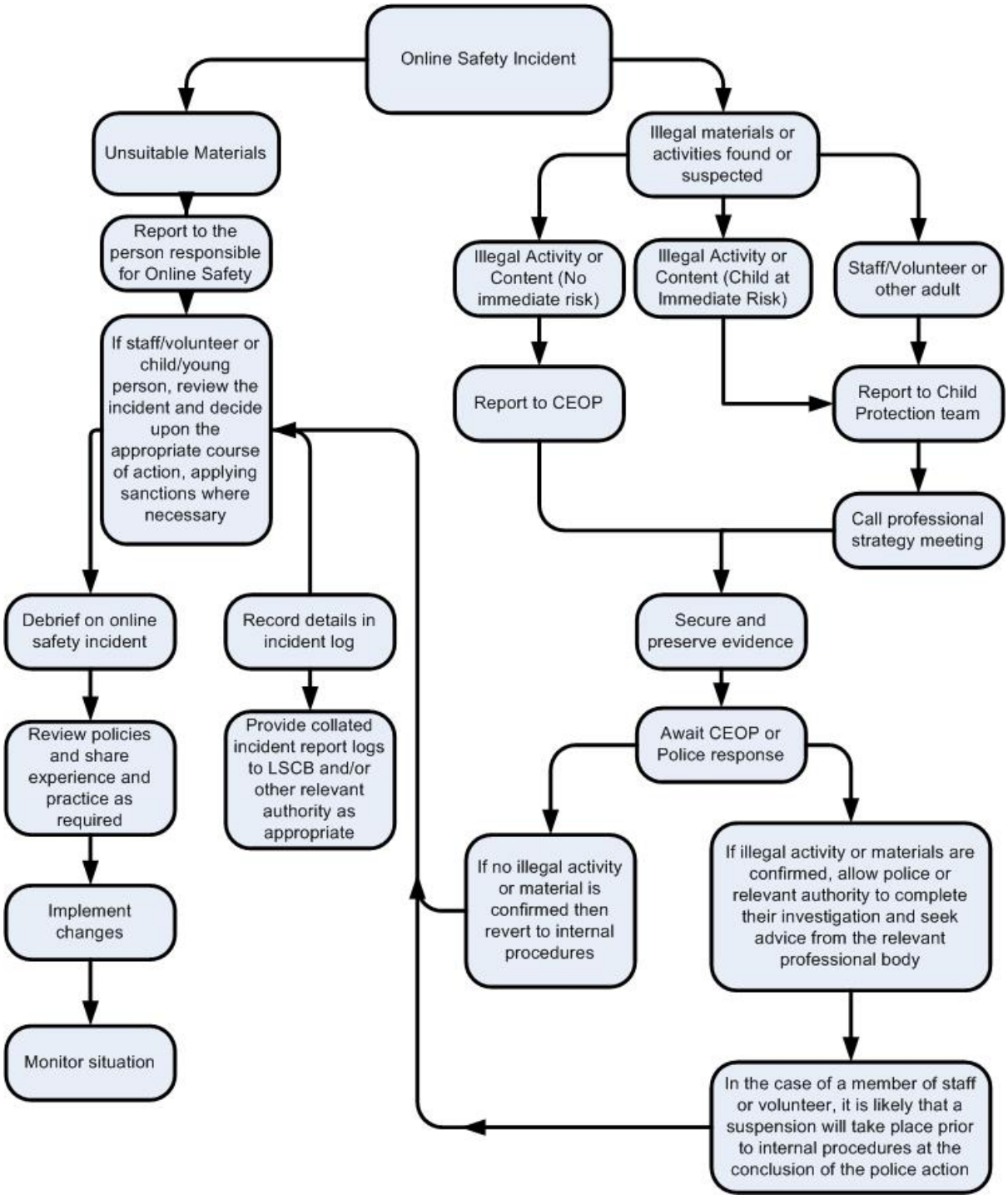
Name of Student	
Signed	
Date	

Appendix C - Responding to incidents of ICT misuse – flow chart

Taken from: South West Grid for Learning - http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Illegal Incidents

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



Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

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

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

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

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

Appendix C(a) - Responding to incidents of ICT misuse – recording notes

Record of reviewing devices / internet sites (responding to incidents of misuse)

School	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Appendix D – Guidance Notes

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

		Acceptable	Acceptable at certain times	Acceptable with supervision	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**						X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.						X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008						X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986						X
	pornography					X	
	promotion of any kind of discrimination					X	
	threatening behaviour, including promotion of physical violence or mental harm					X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					X	
Using school systems to run a private business						X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy						X	
Infringing copyright						X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						X	
Creating or propagating computer viruses or other harmful files						X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)						X	
On-line gaming (educational/social programme)			X				
On-line gaming (non educational)						X	
On-line gambling						X	
On-line shopping / commerce						X	
File sharing						X	
Use of social media			X				