THE KING'S SCHOOL
CHESTER

Online Safety Policy

Policy Owner	**Pastoral Deputy Head**
Last reviewed by Date	Pastoral Deputy Head April 2023
Last approved by Date	Safeguarding Committee June 2023
Next policy review by owner *(annual)*	Pastoral Deputy Head April 2024
Next policy approval by governors *(annual)*	Safeguarding Committee June 2024 Full Board Annual Safeguarding Review October 2024
Circulation	All staff and governors, school website
Related policies	Child Protection and Safeguarding Policy Anti-Bullying Policy Behaviour Policy ICT Acceptable Use Policy - Pupils ICT Acceptable Use Policy - Staff Cyber Security Policy

Contents

Appendices

The Online Safety Policy is in place so that we can best educate, support and protect all members of the King's School community; pupils, staff and parents.

1. Aims

- To provide an overview of all aspects of safe ICT and computer use within the school
- To ensure that we have a consistent approach throughout the school to educating pupils in online safety
- To help protect pupils from the dangers involved in using the internet.

This Online Safety policy has been developed with input from;

- Headteacher
- Governors
- DSL
- Staff – including Teachers, Support Staff, Technical staff
- Pupils

The school will monitor the impact of the policy using:

- Review of issues relating to the use of digital technology – Deputy Head Pastoral/SLT/Online safety group
- Logs of incidents resulting in disciplinary measures - Deputy Head Pastoral/Online safety group
- Monitoring logs of internet activity/filtering (websites and keywords) - IT Support Department
- Internal/External monitoring data for network activity - IT Support Department
- Surveys/questionnaires of
  - students
  - parents/carers
  - staff

2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents /carers and visitors) who have access to and are users of school digital technology systems, both in and out 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/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

3. Roles and Responsibilities

3.1 **Governors** are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving information about online safety incidents and monitoring reports. Through their Safeguarding role, the Safeguarding Governor fulfils this role through:

- Regular meetings with the DSL
- Reviewing of online safety incidents
- Reporting to relevant Governors' meeting

3.2 **The Headteacher** has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the DSL.

The Headteacher and other members of the KLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or a breach of school cyber security.

3.3 **The Designated Safeguarding Lead** is specifically aware of the potential for serious child protection and/or safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

The DSL also chairs the Online Safety Group and is the Online Safety Officer. The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy and other related policies, including the impact of initiatives. The DSL understands the filtering and monitoring systems in place.

3.4 The **ICT Support Department** is responsible for ensuring:

- that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack
- that the *school* meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied on school devices and the school network and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet access / Learning Platform / remote access / email is monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Online Safety Officer for investigation
- that monitoring software/systems are implemented on school devices and the school network and updated as agreed in school policies
- that external penetration testing is carried out regularly to ensure integrity of school systems

3.5 **Teaching and Support Staff** are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read and understood the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher and Deputy Head Pastoral for investigation
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- they monitor the use of digital devices, VPNs, mobile devices, cameras etc in lessons and other school activities and implement current 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

3.6 Pupils

Pupils are responsible for using the school digital technology systems in accordance with the Pupil ICT Acceptable Use Policy and need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Pupils will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.

Finally, pupils 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

3.7 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website /Learning Platform and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of their children's personal devices in the school

4. Education & Training in Online Safety

4.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is be broad, relevant and provides progression, and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are helped to understand the need for the **Pupil ICT Acceptable Use Policy** and are encouraged to adopt safe and responsible use both within and outside school.

  (*detailed in **Appendix 1)***

Staff 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 are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg 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 have clear reasons for the need.

4.2 Staff

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy, Staff Acceptable Use Policy and other associated policies. It is expected that some staff will identify online safety as a training need within the personal development process (PDP).
- The Deputy Head Pastoral (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented and discussed by staff in staff INSET days.
- The Deputy Head Pastoral (or other nominated person) will provide advice/guidance/training to individuals as required.

4.3 Governors

Governors should be briefed on online safety and cyber security measures, with particular importance for those who are members of any group involved in technology/online safety/safeguarding. This may be offered in a number of ways including participation in information sessions for Governors.

4.4 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, web site, Learning Platform
- Parents evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

5. 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. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements, as outlined in the following linked policies;

KSC Technical Security Policy, covering;

- Technical Security measures
- Password Security
- Filtering
- Monitoring

KSC Cyber Security Policy, covering;

- Overview of known threats
- Consequences of cyber breaches
- The schools approach
- Responsibilities

KSC Storage Policy, covering;

- Overview of data storage facilities and procedures implemented to control and manage data within the school
    - Internal network storage
    - Cloud based storage
    - Paper records
    - School archives

6. 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. Use of these mobile technologies should be consistent with and inter-related to other relevant school polices including but not limited to the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy and the Acceptable Use Policies. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

The school Acceptable Use Policies for staff and pupils will consider the use of mobile technologies

The school allows:

	School Devices			Personal Devices	
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	Yes	Yes
Full network access	*Yes*	*Yes*			
Internet only			*Yes*	*Yes*	*Yes*

While the school ***Acceptable Use Policies*** for staff and pupils covers use of mobile technologies within the school, additional policies and guidance documents are available for the management of school owned / provided devices;

A ***Student Device Provision***, covering;

- What we provide
- Why we provide a device
- When students are entitled to a school provided device
- Associated costs
- Ownership

A ***Staff Device Allocation Policy***, covering;

- Eligibility requirements
- Security
- Ownership
- Use of personal devices

A ***Staff Mobile Phone Allocation Policy***, covering;

- Eligibility requirements
- Security
- Usage
- Use of personal mobile devices

7. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

Two levels of parental consent can be given when a pupil enters the school. Parents can consent to the image and full name being used or published on the school website / social media / local press, or just image with no personal details. Parents can consent to no use.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

If you have given permission for your child's image to be used, we will not ask express permission from pupils every time we take a photo or video. However, we do tell pupils what the image is being used for and we will consider the child's opinions over the age of 13 and they can opt out.

- Parents are free to take photographs/moving images at any event as long as this is for personal use and is not used in a public arena, such as social media channels, websites, publications etc. Parents are not permitted to take photographs of other pupils without the prior agreement of that pupil or the pupil's parents. No photos can be taken in the swimming pool, changing rooms or backstage.
- On occasions, such as play or concert, parents may be directed not to take photos or video. Copyright issues may prevent parents recording or taking photographs of some plays or concerts. Parents will be made aware of this before any performance starts.
- The school reserves the right to refuse or withdraw permission to film or take photos (at a specific event or more generally) if any parent who does not follow these guidelines.

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.

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.

Pupils must not take, use, share, publish or distribute images of others without their permission

8. Data Protection

This is covered by the school's ***Data Protection Policy***, supported by the ***Data Retention Policy***

9. Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Social Media

Social Media usage is covered within the ***Staff Technology Acceptable Use Policy***

The school aims to provide a safe learning environment for pupils and staff.

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

- Ensuring that personal information is not published without consent
- Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

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

Monitoring of Public Social Media:

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- The school will effectively respond to social media comments made by others according to a defined policy or process
- The use of the school’s social media channels for professional purposes is monitored by the marketing department.

Appendix 1: Online Safety Education

1.1 Removes induction (and induction of chance entry pupils)

- Tutor goes through
- The content of the Pupil ICT AUP
- Use of school network– username, password, changing passwords, password security, email account, Firefly.
- Use of MS Teams – navigation, assignments, remote lessons, chat function.
- Use of OneNote – copying pages from content library, uploading work, recording voice (MFL).

1.2 Senior School Pastoral programme and PSHE programme

	Pastoral Programme	PSHE	Other
Removes	About different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help.	Online safety and risks of sharing of consensual and non-consensual nudes. Online legislation and consequences.	Take part in National Anti-Bullying Week activities and Safer Internet Week activities (all year groups)
	About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.		Information displayed on screens around school during Safer Internet Awareness Week (all yr groups)
Shells	How to observe online etiquette and the peer pressure associated with online bullying and gaming.		
Third Year	How to identify harmful behaviours online (including bullying, abuse, pornography or harassment) and the peer pressure associated with online bullying.	Sharing consensual and non-consensual nudes. Social media influences.	
4th Year	How social media can offer opportunities to engage with a wide variety of views on different issues if used responsibly and your online profile.		

5th Year	Online misconceptions and the dangers of this. Sharing of consensual and non-consensual nudes.		
Sixth Form	The importance of protecting their own and others’ reputations; protecting their ‘online presence’: the concept of having a personal ‘brand’ that can be enhanced or damaged. Plagiarism using online platforms.		

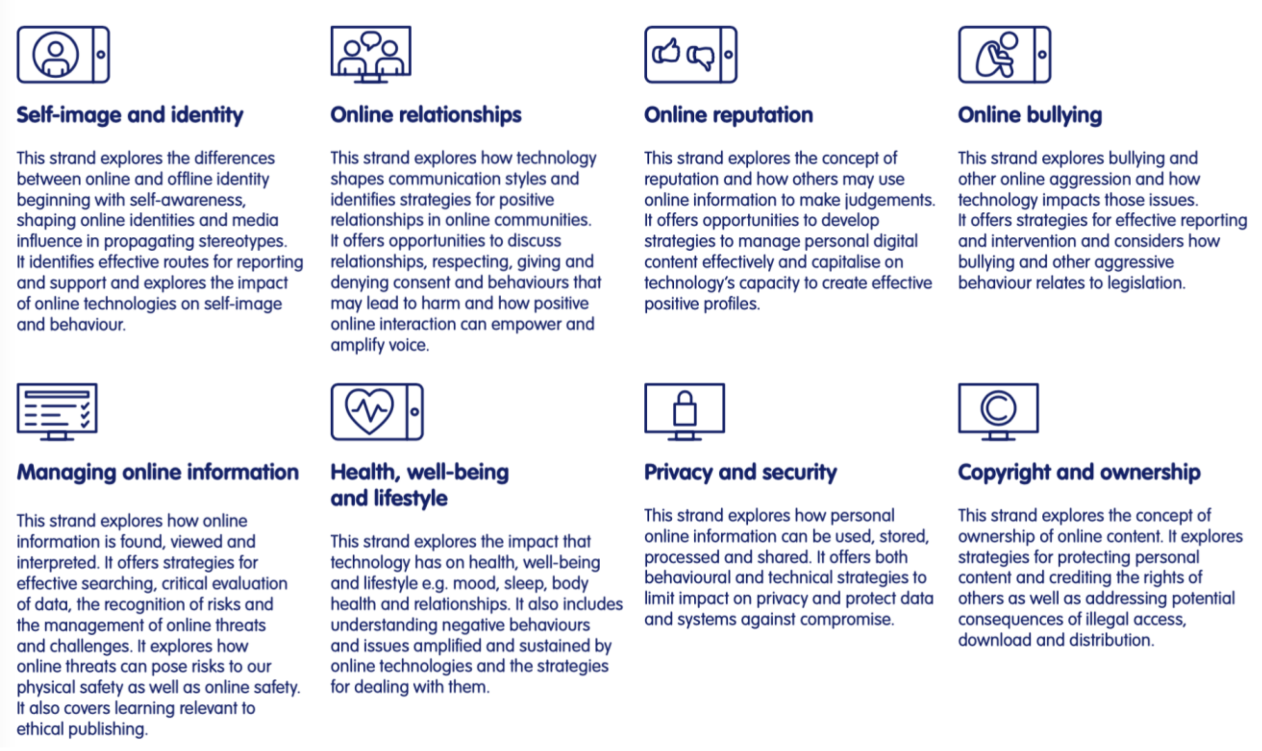
1.3 Online Safety in KS3/KS4 Computer Science

At King’s School we want to ensure that we are following best practice to provide students with understanding of Online Safety and Digital Citizenship to equip them for digital life.

This follows the “Education for a Connected World” produced by the UK Council for Internet Safety - https://www.gov.uk/government/publications/education-for-a-connected-world

All students receive two Computer Science lessons a fortnight in Removes and Shells. Some students who have opted for the subject take the subject in 3rd year and above.

The Framework breaks down the area into eight strands:



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology’s capacity to create effective positive profiles.

Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

Some of these strands will be covered in PSHE and the pastoral programme, but in Computer Science we try and make sure we cover as much as possible in Removes and Shells.

Many of the resources are adapted from those provided by Common Sense Education - https://www.commonsense.org/education/uk/digital-citizenship/secondary

The following lessons are covered in Computer Science

Strand	Topic & learning objectives.	Year Group
Privacy and Security	"How secure are your passwords?" ● Understand why we need logons & passwords ● Understand what makes a 'good' password ● Be able to come up with strong unique passwords	Removes
Online relationships	"Chatting Safely Online" ● Analyse how well they know the people they interact with online. ● Reflect on what information is safe to share with different types of online friends. ● Learn to recognise red flag feelings and use the "Feelings & Options" thinking routine to respond to them.	Removes
Online bullying	"Is it cyberbullying?" ● Recognize similarities and differences between in-person bullying, cyberbullying, and being mean. ● Empathize with the targets of cyberbullying. ● Identify strategies for dealing with cyberbullying and ways they can be an upstander for those being bullied.	Removes
Online reputation	"The power of digital footprints" ● Define the term "digital footprint" and explain how it can affect their online privacy. ● Analyse how different parts of their digital footprint can lead others to draw conclusions -- both positive and negative -- about who they are. ● Use the Take a Stand thinking routine to examine a dilemma about digital footprints.	Removes
Health, well-being and lifestyle	"Finding balance in a digital world" ● Reflect on their common online and offline activities. ● Identify ways to "unplug" to maintain balance between online and offline activities. ● Use the "Digital Habits Check-up" routine to create a personal challenge to achieve more media balance.	Removes
Managing Online Information	"Don't Feed the Phish" ● Compare and contrast identity theft with other kinds of theft ● Describe different ways that identity theft can occur online ● Use message clues to identify examples of phishing	Shells
Health, well-being and Lifestyle	"Digital Media and your brain" ● Explore ways that different types of digital media are, and aren't, designed to help us make good media choices. ● Reflect on how digital media is designed to either help or hinder the addition of meaning and value in our lives. ● Think about how to develop good, healthy habits when using digital media.	Shells

Online Relationships	"Digital Drama Unplugged" • Reflect on how easily drama can escalate online. • Identify de-escalation strategies for dealing with digital drama • Reflect on how digital drama can affect not only oneself but also those around us.	Shells
Online relationships	"My social media life" • Identify the role of social media in students' lives. • Reflect on the positive and negative effects social media use has on their relationships. • Recognize "red flag feelings" when using social media and use the Feelings & Options thinking routine to consider ways to handle them.	Shells
Online relationships	"When things go too far - extreme behaviour online" • Understand what we mean by "Extremism" or "Radical views" • Be able to recognise factors that might make someone susceptible to radicalisation • Understand what can happen to people who have been radicalised.	Shells
Managing Online Information	"Being aware of what you share" • Reflect on the concept of privacy, including what they feel comfortable sharing and with which people. • Analyse different ways that advertisers collect information about users to send them targeted ads. • Identify strategies for protecting their privacy, including opting out of specific features and analysing app or website privacy policies.	Shells

The following strands are covered in Computer Science as an option to Thirds and above:

Strand	Topic & learning objectives.	Year Group
Privacy and Security	Introduction to cyber security Introduction to malware Security measures Penetration, testing and hackers	Third Year
Privacy and Security	Forms of attack Understanding brute force attacks Data interceptions and threats Threats from malware Understanding denial of service attacks Understanding SQL injection	Fourth Year Fifth Year
Managing Online Information	Understand what is meant by social engineering	Third Year Fourth Year Fifth Year
Managing Online Information	Understanding phishing Identifying and preventing vulnerabilities Legal and cultural and environmental issues of computer science	Fourth Year Fifth Year

1.4 Online Safety in the Junior School

Online safety in the Junior School is delivered through termly assemblies delivered by the JS prefects. Topics are centred around an understanding of gaming, safe use and its dangers and responsible mobile phone use. Safer Internet Day (each February is a focus day every year with activities prepared and delivered by all JS teachers in collaboration with the UK Safer Internet Day website.

Through the 'Celebrating Difference' and 'Relationships' Jigsaw strands in PSHE, students in the Junior School also explore types of bullying online, safety within the online community, being in an online community and online gaming.

1.5 Online Safety in Willow Lodge

Online safety in Willow Lodge is delivered through class topics, school and class assemblies and on special days such as Internet Safety Day. Topics are centred around safety when playing games on computers / tablets and how to get help if they need it. Safer Internet Day (each February) is a focus day every year with activities prepared and delivered by all class teachers in collaboration with the UK Safer Internet Day website. Educative videos and stories are shared with the youngest children in Reception.

Appendix 2: Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. 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.

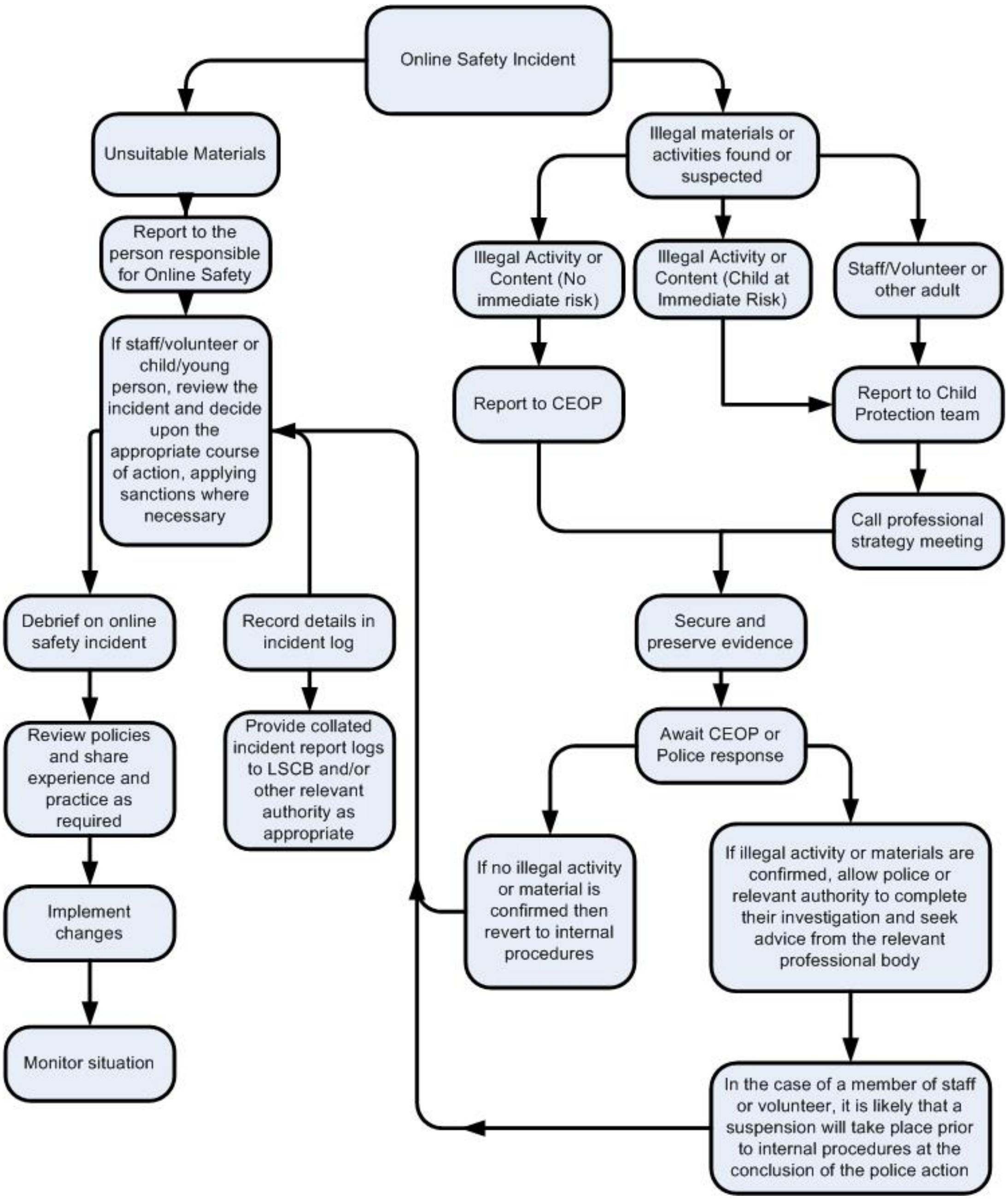
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems.

The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					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	X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gambling					X	
File sharing ???		X				
Use of social media			X			
Use of video broadcasting e.g. YouTube			X			

2.1 Responding to incidents of misuse which may include illegal incidents

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


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

2.2 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school 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 national / local organisation
- ▪ Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

Appendix 3: School Actions & Sanctions

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 disciplinary procedures as follows:

Pupils Incidents	Refer to tutor	Refer to Head of House	Refer to Deputy Head Pastoral/DSL	Refer to Police	Refer to technical support staff for	Internal sanction	Inform parents / carers	Temporary exclusion
Deliberately accessing or trying to access material that could be considered illegal	X	X	X	X	X		X	X
Unauthorised use of non-educational sites during lessons	X	X			X	X		
Unauthorised / inappropriate use of mobile phone camera/ digital camera / other mobile device to capture images	X	X				X	X	
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X				X	X	
Unauthorised downloading or uploading of files	X	X			X	X	X	
Allowing others to access school network by sharing username and passwords	X	X				X	X	
Attempting to access or accessing the school network, using another pupil's account	X	X				X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X		X	X
Corrupting or destroying the data of other users	X	X				X		
Sending an email, text, message or post that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X				X	X