THE
KING'S SCHOOL
CANTERBURY

Online Safety Policy

Responsible Person: Designated Safeguarding Lead

Latest Review Completed: September 2022

What is Online safety?
Information and Communications Technology (IT) is now an essential education tool. With its benefits come dangers. This means we now must think beyond the traditional school environment when ensuring every student's safety. Once the desktop computer was the only way to access the internet, now many mobile phones and games consoles offer broadband connections. Students now work online in school and at home and have personal devices not covered by network protection. Therefore, the emphasis everyone needs to understand the risks and act accordingly.

Unfortunately, there are times when Internet use can have a negative effect on children. Students, staff, parents and carers should be aware of the potential dangers and take measures to ensure safe usage of technology.

Introduction
IT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing a significant role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment.

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

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

Whilst exciting and beneficial both in and out of the context of education, internet technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At The King's School, we understand the responsibility to educate our students on online safety issues, teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in and beyond the context of the classroom. Both this policy and the Acceptable User agreements are inclusive of both fixed and mobile internet technologies provided by the school, such as PCs, laptops, personal digital assistants (PDAs), tablet PCs, webcams, whiteboards, voting systems, digital video equipment, digital cameras, visualisers, etc. and technologies owned by students and staff brought onto school premises, such as laptops, mobile phones etc.

Policy Aims
This Online Safety Policy combines the Kent County Council (KCC) Online safety Policy template with specialist advice and input as required. It takes into account the DfE statutory guidance Keeping Children Safe in Education (KCSIE) 2022, and the Kent Safeguarding procedures as set out by the Kent Safeguarding Children Multi-Agency Partnership Arrangements (KSCMP)

The purpose of the Online safety Policy is to:
- Safeguard and protect all members of the school community online.
- Identify approaches to educate and raise awareness of Online safety through the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to Online safety concerns.

Links with other Policies and Practices
This policy should be read alongside other relevant policies, practices and actions plans including:
Anti-bullying policy, AUPs and codes of conduct, Behaviour and Discipline policy, Safeguarding and Child protection policy. Curriculum policies, such as: Digital Curriculum, Computer Science and Life Matters. Data Protection procedure, taking, storing and using images policy, Mobile phone policy and social media, website and publication guidelines, Searching, screening and confiscation policy.

Roles and Responsibilities
As online safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are upheld. The school recognises that all members of the community have important roles and responsibilities to play regarding online safety.

Senior Leadership team
The SLT will:
- Ensure online safety is viewed as a safeguarding Issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the security system embedded within the school's systems and networks.
- Ensure online safety is embedded within the progressive whole school curriculum which enables students to identify risks as well as protect themselves from the dangers they may face online.
- Support the DSL, and Safeguarding Team, to ensure they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure appropriate risk assessments are undertaken regarding the safe use of technology.

The Safeguarding Team
The school has an allocated member of the Safeguarding Team whose main responsibility is online safety/ E-Safety (Mr. Matt Thornby). This member of staff will:

- Act as named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies as appropriate.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure members of staff receive regular, up-to-date and appropriate online safety training.
- Ensure that online safety is promoted to students, staff and parents through various outreach programs.
- Maintain records of online safety concerns.
- Monitor online safety incidents to identify gaps and trends, and use this data to update education response, policies and procedures.

All Staff
It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies and procedures.
- Read and adhere to the Online Safety Policy.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice both in professional and personal settings when using technology, both on and off site.
- Embed online safety in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety dangers that their student may face.
- Identify online safety concerns and take appropriate action by following the reporting procedures stated in the Safeguarding Policy.

All students
It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age-appropriate online safety educational opportunities.
- Read and adhere to the school's Online Safety Policy and expectations.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

Parents/Guardians/Carers

The school recognises that parents, guardians and carers have an essential role in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership with caregivers by:

- Providing information and guidance on online safety
- Drawing their attention to the Online Safety Policy and expectations in newsletters, letters, the prospectus and on the website.
- Requesting they read the online safety information as part of joining the school.
- Requiring them to read The School AUP and discuss its implications with their children.

Password Security
Password security is essential for students and staff, particularly for staff as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and accept an Acceptable Use Agreement (AUPs) to demonstrate that they have understood the school's Online Safety Policy.
- Users are provided with an individual network log-in. They are also expected to use a personal password and keep it private.
- Students are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password, report this a member of staff.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and data and ISAMs, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Under no circumstances are staff allowed to let any other person use their username and password. This could result in disciplinary action.

Managing Online safety within School
The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites and materials before use.
- Staff will not avoid discussions and the research of terrorism as this may be relevant to the lesson being taught. Instead, staff should consider appropriate guidance to ensure that the material being accessed is relevant and appropriate.
- Raw image searches are discouraged when working with students.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- At present, the school endeavours to deny access to social networking sites to students within school.

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

Students, Parents and Carers

- All students are advised to be cautious about the information given by others on sites. This is because other people may not be who they claim to be.
- Students, parents and carers are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students, parents and carers are always reminded to avoid giving out personal details on such sites which may identify them or their location (full name, address, mobile/home phone numbers, school details, IM/email address and specific hobbies/interests).
- Students, parents and carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students, parents and carers are asked to report any incidents of online bullying to the school.
- The school advises parents and carers to locate PCs and laptops in a highly visible part of the home, which can be regularly monitored.
- Students should not meet anyone that they have met through the internet, unless accompanied by a trusted adult.

School Staff

- If you are a member of a social networking site (e.g. Facebook, Instagram, Twitter, Snapchat, Tik Tok) ensure that your security settings are high.
- Staff who are members of social networking sites must not accept past and current students as friends for at least a period of 3 years after the student has left school and not before the student is 19 years of age.
- Staff are advised to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- School laptops are only to be used by the staff member allocated the laptop. The laptop should not be used by family members and should only be used for work purposes and not for personal use.
- Under no circumstances should staff take any images and videos taken within the school environment off site without the authorisation of the Head or the delegated deputy, school issued mobile devices have been made available for such occasions where the taking of video or images are necessary to support the work of the school.

Mobile technologies (including mobile phones)

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Student Mobile devices

- Students are allowed to bring personal mobile devices/phones to school as a safety precaution for travelling on and offsite for their timetabled lessons. Students are encouraged to keep important contact numbers on their phone in case of emergencies (ie. Matrons/Pastoral Care Assistants, Housemistress/masters, Safeguarding Team).
- Upon arrival to lessons, students are expected to place their mobile phones in the allocated box/tray to avoid disruption during the lesson.
- If a teacher has decided that student mobile phone use is necessary for a specific task within a lesson, then students will be clearly informed when and for what purpose they are permitted to use their mobile phone and must only use the mobile phone for the identified period.
- The sending of inappropriate text messages, pictures or content between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.

Staff Mobile Devices

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device except in the case of an emergency.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages, pictures or content between any members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices

- The sending of inappropriate messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as laptops and PDAs for off site visits and trips, only these devices should be used.

Managing Email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. All members of the school community are provided with a school email address and are expected to use this email address responsibly. The school expects all communication through emails to be professional and age appropriate regardless of whether the communication is between students and/or staff. To ensure that the school email platform is appropriately used, all members of the school community must adhere to the rules and expectations stated in the school AUPs.

The King's School:

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoid the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged and if necessary, email histories can be traced.
- Only the school provided email account should be used for school business.
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Students must immediately tell a teacher/trusted adult if they receive an offensive email.
- Staff must inform the Safeguarding Team with responsibility for online safety/line manager if they receive an offensive email.

Safe Use of Images and Film
Digital images are easy to capture, reproduce and publish and therefore could be misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of students), the school permits the appropriate taking of images by staff and students with school equipment under the following guidance.

At The King's School:

Staff
- Staff must never take images or make videos of students covertly on any digital device
- Any images or videos that are made, must be for teaching and learning purposes.
- Staff that wish to take photographs or videos with their students as a keepsake, may do so in certain circumstances:
    - It should be declared to a senior member of staff.
    - The images / videos should never be taken covertly and always with the full consent of the students.
    - Should not be shared online or any social media account except for on official school media accounts.
    - Should always be appropriate and not used to undermine or embarrass a student.

Parents
- Will be allowed to film and take images of their child during performances/sporting fixtures but will be reminded at the beginning of any performance/ sporting fixture that any image or video taken must not be shared online or on any social media account as other students may also be included in such material.
- Will not be allowed to film or take images of their child during any cathedral services.

Students
Students are not permitted to use personal digital equipment, including mobile phones and cameras to record images of the students or staff within the school environment or when on field trips unless pre-approved by a member of staff.

Social Media

See separate policy Social Media Website and Publication guidelines.

Social media provides a fantastic opportunity for students, staff, parents and carers to connect to other members of the school community and wider friends and family regardless of geographic location. Whilst social media has many benefits, the school recognises that these websites and apps provide a greater platform for inappropriate, negative, and unacceptable behaviours which could have detrimental effects on members of our school community. The expectations regarding safe and responsible use of social media applies to all members of the school community.

Staff

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal, or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Some things to consider are:
    - Setting the privacy levels of their personal sites as strictly as possible and reviewing them regularly.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as those of the school.

- Members of staff are encouraged not to identify themselves as employees of the school on their personal social media networking accounts. This is to prevent information on these sites from being linked with the school, to safeguard the privacy of staff members and prevent outsiders from accessing students.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify a member of SLT immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils, parents, and guardians

- All members of staff are advised not to communicate with or add as "friends" any current or past pupils or current or pass pupils' family members via any personal social media sites, applications, or profiles.
- Any pre-existing relationships or expectations that may compromise this will be discussed with the DSL and/or the Head.
- If ongoing contact with a pupil is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents/carers nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Head.

- Any communication from pupils and parents received on personal social media accounts should be reported to the schools DSL.

Official Use of Social Media
Official social media channels are managed by the Head of Marketing and no official channels can be established without discussion with them. Official social media channels have been set up as a distinct and dedicated social media sites or accounts or education or engagement purposes only. The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
- Sign the school's social media AUP.
- Be professional at all times and be aware that they are an ambassador for the school.
- Disclose their official role and/ or position but make it clear that they do not necessarily speak on behalf of the school.
- Be responsible, credible, fair, and honest at all times and consider how the information published could be perceived or shared.
- Always act within the legal framework they adhere to within the workplace.
- Ensure they have appropriate written consent before posting images on the official social media channel.
- Not disclose information, make commitments, or engage in activities on behalf of the school unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, pupils, parents or carers.
- Inform their line manager, the DSL and/or the Head of any concerns, such as criticism, inappropriate content or contact from pupils.

Students
- Safe and appropriate use of social media will be taught to pupils as part of embedded and progressive education approach, via age-appropriate sites and resources
- Any concerns regarding pupils' use of social media, both at school and at home, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites of tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communication and report concerns both within school and externally.

Safeguarding
Although the use of IT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to risk of harm. Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well-being of children may also exist in a variety of other ways.

Grooming & Online Child Sexual Abuse and Exploitation
It is known that adults who wish to abuse children may pose as children to engage and then meet up with the young people they have been in communication with. This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones. An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out.

Cyberbullying
Increasingly bullying is conducted on the internet or by the use of messaging platforms and is therefore harder for schools to notice and deal with. As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include changes in children's behaviour, demeanour, physical appearance and presentation, language, or progress.

Sending and receiving sexual content (sexting)
Sexting means sending indecent images (pictures and/or videos) of yourself or others or sending sexually explicit messages. Sexting is commonly known as "trading nudes," "dirties" or "pic for pic." Sexting can happen on any electronic device that allows sharing of media and messages including smartphones, tablets, laptops, or mobiles.

Indecent images of Children (IIOC)
Taking, making, sharing and possessing indecent images and pseudo-photographs of people under 18 is illegal. A pseudo-photograph is an image made by computer-graphics or otherwise which appears to be a photograph. The school will take action regarding IIOC on school equipment and/or personal equipment, even if the access took place off site.

The school is aware that some pupils are considered to be more vulnerable online due to a range of factors. The school will seek input from specialist staff as appropriate, including the SENCO and Safeguarding Team.

Reporting a concern about a student
If you are concerned about a student's safety for any of the following reasons, a concern must be reported as stated in the Safeguarding and Child Protection Policy:

- **CONTENT**: Being exposed to illegal, inappropriate, or harmful material.
- **CONTACT**: Being subjected to harmful online interactions with other users.
- **CONDUCT**: personal online behaviour that increases the likelihood of, or causes, harm

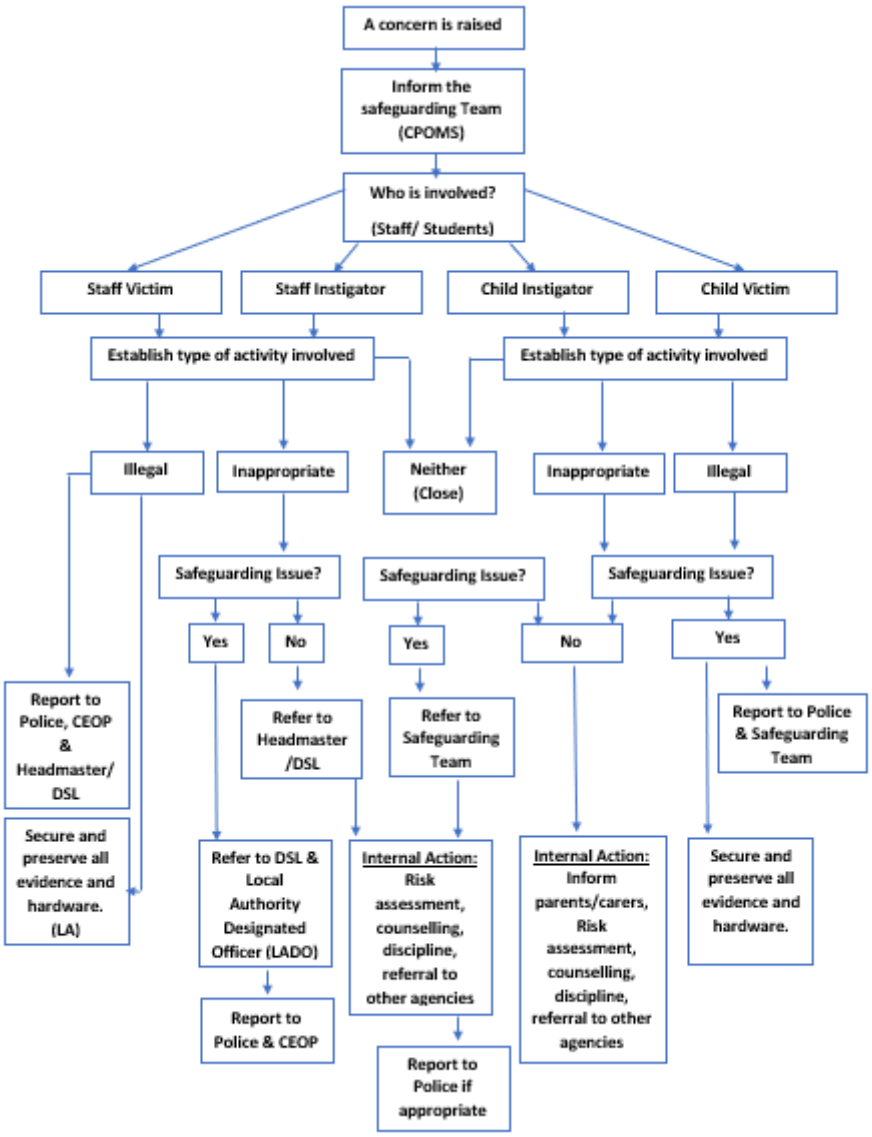
Concerns regarding a student's online safety are reported the same as any other concern. Staff should report the concern on CPOMs within 24 hrs. unless there is an imminent threat to the student's safety and wellbeing – in which case, you must stay with the student until a member of the Safeguarding Team can relieve you.

Misuse and infringements of computer equipment or mobile technologies that breach any of the guidelines set out in the Online safety Policy or AUP's may result in disciplinary action for both staff and students.

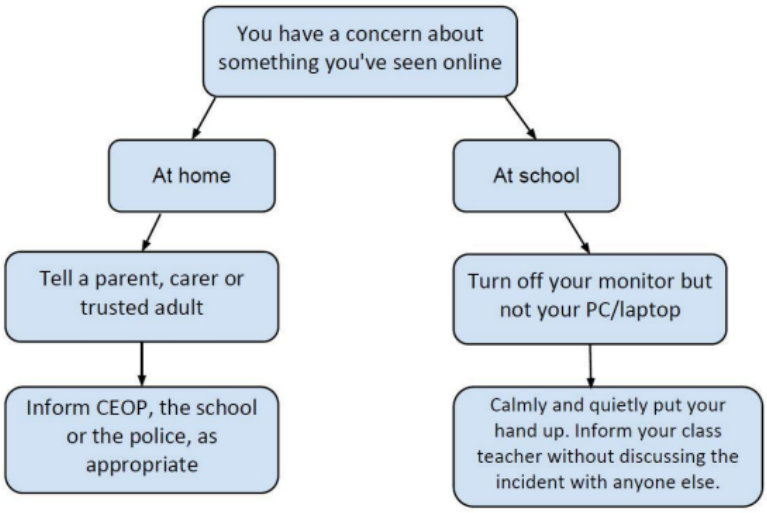
For more information on the reporting of a concern, please refer to the Safeguarding Policy or speak to a member of the Safeguarding Team.

Students and staff should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Staff Flow Chart for Concerns



Student Flow Chart for Concerns



Appendix One: Live Learning Protocols

Due to COVID- 19 and the possibility of another local or national lockdown, The King's School have added this appendix to the policy should the school require to provide an online or "hybrid" education platform to their students at any point in the future.

Staff Protocols for live learning

- All live sessions must be held via established and provided school technologies, platforms and systems (ie. Microsoft Teams).
- Staff must ensure that secure links for their respective lessons are not shared with students outside of their groups. Staff should only provide the link required for their session into any communication with students.
- Staff must use these secure links to ensure that the ability to "mute" and "remove" students from the live session is retained.
- Staff must ensure that they log in to the live session promptly at the scheduled start time. This applies to both live subject sessions and live tutorial sessions (if offered).
- At the end of the live session the staff member must remain in the live session until all other participants have left, they can then end the session (staff may force the exit of students in necessary).
- In all cases, staff must ensure that they are appropriately dressed, in line with the staff handbook (and this applies to anyone who may appear on screen).
- In all cases, staff must ensure that the language used is professional and polite (this applies to anyone who may be heard on the microphone).
- Staff must ensure an appropriate background is seen by students especially when delivering an online session from their home. Using the blurred filter/background on some platforms may be desirable.
- A register of attendance must be taken within the first ten minutes of the session starting.
- For safeguarding purposes, both the staff member(s) and all students must have their webcam switched on while the register is taken.
- Where a student's devices does not have a webcam, or the webcam is nonfunctional, staff must use their discretion in ascertaining the true identity of the participant.
- When the attendance register has been completed, students may turn off their webcams off (this is at the teacher's discretion) and must put their microphones on mute (expect when called upon by the staff member to respond)
- There is no expectation for staff to record any online sessions.

If you have any concerns presented during a live lesson, please log the concern via CPOMS which will notify the Safeguarding Team.

Student Protocols for live learning

Students are expected to maintain the high school standards regardless of whether the lesson is delivered in person or online and show respect, kindness and consideration towards both staff students. Any unacceptable language, behaviours, or use of technology will be addressed in line with other policies (Behaviour Policy, Safeguarding Policy, AUPs etc.)

- During live sessions, students must be appropriately dressed and be in an appropriate area of their home (this must not be a bedroom)
- Students must act appropriately during the live sessions, and this includes any other members of the household who are in sight/ sound of the session.
- Students must use appropriate language towards all members of the live session.

- Teachers will manage the sessions like they would their classroom. This means they will decide whether they want webcams to be turned on during the session, whether they mute all participants etc.
- An attendance register will be taken, and non-attendance will be followed up.
- Students will only attend/enter the live session of a group for which they are a member. Disruption of other sessions will result in disciplinary action.
- Any misuse of webcam or other devices will result in disciplinary action.
- Taking photographs or screenshots of the screen is strictly forbidden.