THE
KING'S SCHOOL
CANTERBURY
JUNIOR KING'S

Online Safety Policy

The policy is applicable across the whole school, including EYFS

Responsible Person: Designated Safeguarding
Latest Review Completed: September 2026

What is Online Safety?

Information and Communications Technology (ICT) is 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. Pupils 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. Pupils, staff, parents and carers should be aware of the potential dangers and take measures to ensure safe usage of technology.

Introduction

ICT 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.

ICT 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 ICT 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 Junior King's Canterbury, we understand the responsibility to educate our pupils 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 Use Agreements are inclusive of both fixed and mobile internet technologies provided by the school, such as PC's, laptops, personal digital assistants (PDAs), tablet PCs, webcams, whiteboards, voting systems, digital video equipment, digital cameras, visualisers, etc. and technologies owned by pupils 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) 2025, 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.
- Ensure appropriate filtering and monitoring systems are in place. These are in line with filtering and monitoring standards published by: the Department for Education.

Links with other Policies and Practices

This policy should be read alongside other relevant policies, practices and actions plans including:

Anti-bullying policy, AUP's and codes of conduct, Behaviour and Discipline policy, Safeguarding and Child protection policy. Curriculum policies, such as: Digital Curriculum, Computer Science and RSE. Data Protection procedure, taking, storing and using images policy, Mobile device and Smartwatch policy and social media, website and publication guidelines, Searching, screening and confiscation policy.

Roles and Responsibilities

Governing Body Responsibilities

The Governing Body has strategic oversight of online safety and safeguarding. This includes:

- Ensuring that appropriate policies, procedures, and systems are in place
- Receiving regular safeguarding reports, including online safety trends and incidents

- Providing challenge and support to ensure the effectiveness of filtering, monitoring, and education
- Ensuring compliance with statutory safeguarding guidance

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 pupils 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 fulfill 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 King's school has an allocated member of the Safeguarding Team whose main responsibility is Online Safety/E-Safety (Mr. Matt Thornby), he has completed CEOPS Ambassador training. Liaising with the DSL at Junior King's, Canterbury. 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 pupils, 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 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.
- New staff, volunteers, and governors receive online safety guidance as part of induction.
- Training is regularly updated to reflect emerging risks, including social media, online harm, and artificial intelligence.
- Staff are expected to read and understand this policy and the Acceptable Use Agreement (AUP).

All pupils

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 pupils 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 pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for

password security.

- All users read and accept an Acceptable Use Agreement (AUP's) 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.
- Pupils 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, ISAMs and CPOMS, 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 pupils 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 pupils.
- 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 pupils within school.

Filtering and Monitoring

The School has appropriate **filtering and monitoring systems in place** to safeguard pupils and staff online. These systems are regularly reviewed to ensure they remain effective and proportionate.

- The IT Lead is responsible for the day-to-day operation of filtering and monitoring systems.
- The DSL and Safeguarding Team oversee safeguarding implications and ensure that alerts are managed appropriately.
- Filtering and monitoring systems are reviewed at least termly, and following any safeguarding incident or emerging risk.
- Alerts generated by monitoring systems are reviewed promptly and, where appropriate, recorded on CPOMS and managed in line with safeguarding procedures.
- The School ensures that filtering is appropriate to the age and stage of pupils, while not unreasonably limiting educational access.
- The effectiveness of systems is reported to Governors as part of safeguarding oversight.

The School follows the Department for Education's guidance on filtering and monitoring and ensures systems are fit for purpose and regularly updated**.**

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 pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Pupils, Parents and Carers

- All pupils 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.
- Pupils, 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.
- Pupils, 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).
- Pupils, parents and carers are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils, parents and carers are asked to report any incidents of online bullying to the school.
- The school advises parents and carers to locate PC's and laptops in a highly visible part of the home, which can be regularly monitored.
- Pupils 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 pupils 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

- Selected pupils (boarders, children that travel on public transport, children with specific parental permission) are allowed to bring personal mobile devices/phones to school as a safety precaution for travelling on and offsite for their timetabled lessons. Pupils are encouraged to keep important contact numbers on their phone in case of emergencies.
- Upon arrival to school, pupils are expected to hand in their mobile phones to be stored in the allocated places to avoid disruption during the school day.
- 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 pupils. 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 pupils 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 AUP's.

Junior 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 pupils, 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.

- Pupils should only use school approved accounts for contact with school staff.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive email.
- Staff must inform the Safeguarding Team member 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 pupils), the school permits the appropriate taking of images by staff and pupils with school equipment under the following guidance.

At Junior King's School:

Staff

- Staff must never take images or make videos of pupils 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 pupils 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 pupils.
  - 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 pupils may also be included in such material.

Pupils

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras to record images of the pupils 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 pupils, 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 pupils.
- 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.

Pupils

- In Upper School, 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.

Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) technologies, including generative tools (e.g. ChatGPT) and learning platforms with AI features, may be used to support teaching and learning in age-appropriate ways. When used in school, AI tools must always be accessed under staff supervision and for educational purposes only.

Pupils are taught to understand that AI systems may provide inaccurate or biased information and do not replace human judgement. They are encouraged to use critical thinking when engaging with AI-generated content.

Staff must ensure that any AI tool used with pupils complies with UK data protection regulations and the school's safeguarding policies. Pupils are not permitted to share personal data with AI tools, and AI use is monitored to prevent misuse, including inappropriate content generation or academic dishonesty.

The school is committed to keeping up-to-date with best practices in AI use and educating pupils about its ethical, safe, and responsible application.

Online Safety – Awareness of Risks

The School recognises the vital importance of educating pupils, staff, and the wider school community about the risks associated with online activity. In line with *Keeping Children Safe in Education (KCSIE) 2025*, we categorise online risks into the widely recognised **Four Cs**:

1. **Content** – Being exposed to illegal, inappropriate, or harmful material. This includes:
   - Pornography, violence, extremist material
   - Mis/disinformation, including **fake news and conspiracy theories**
   - Biased or misleading representations of groups, cultures, or individuals
2. **Contact** – Being subjected to harmful online interaction with others. This may involve:
   - Grooming, exploitation, or coercion by strangers
   - Contact with individuals promoting radicalisation or criminal activity
   - Cyberbullying or targeted harassment
3. **Conduct** – Personal online behaviour that increases risk. This includes:
   - Sharing too much personal information
   - Sending or receiving explicit images or messages
   - Engaging in abusive or hurtful communication
4. **Commerce** – Risks linked to online shopping, advertising, and financial scams. This

includes:

- Phishing or fraudulent transactions
- In-game or in-app purchases that exploit children
- Exposure to gambling or loot box mechanisms

All pupils will be taught to identify, understand and respond to these risks through age-appropriate digital literacy and PSHE (Personal, Social, Health and Economic) education. Staff receive regular training to help them recognise warning signs and report any online harms.

The School is also mindful of emerging risks, particularly relating to:

- **Generative Artificial Intelligence (AI)** tools (e.g. AI chatbots, image generators)
- Inappropriate or unfiltered access to AI-based search results or responses
- Peer misuse of AI to bully, deceive, or produce explicit content

We use robust **filtering and monitoring systems** in accordance with the latest DfE guidance, including the *Plan Technology for Your School* toolkit, and follow the DfE's **Product Safety Expectations for Generative AI**.

Parents are supported with guidance and updates to help them engage with their children's online lives and reinforce safe behaviours at home.

Safeguarding

Although the use of ICT 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.

Sharing of Sexual Images (Youth-Produced Sexual Imagery)

The sharing of sexual images or messages by children is a serious safeguarding issue.

This may involve:

- Sending or receiving sexual images, videos, or messages
- Possessing or sharing images of another young person

Creating, possessing, or sharing indecent images of a person under 18 is illegal, even where the individual has consented.

The School will respond to incidents in line with UKCIS guidance and safeguarding procedures. Responses will:

- Be proportionate and child-centred
- Avoid unnecessary criminalisation of pupils
- Consider the age, context, and level of risk
- Involve the DSL and external agencies where appropriate

All incidents will be treated as safeguarding concerns, and handled with sensitivity and confidentiality.

Pupils will be educated about:

- The risks and consequences of sharing images
- How to seek help and report concerns

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.

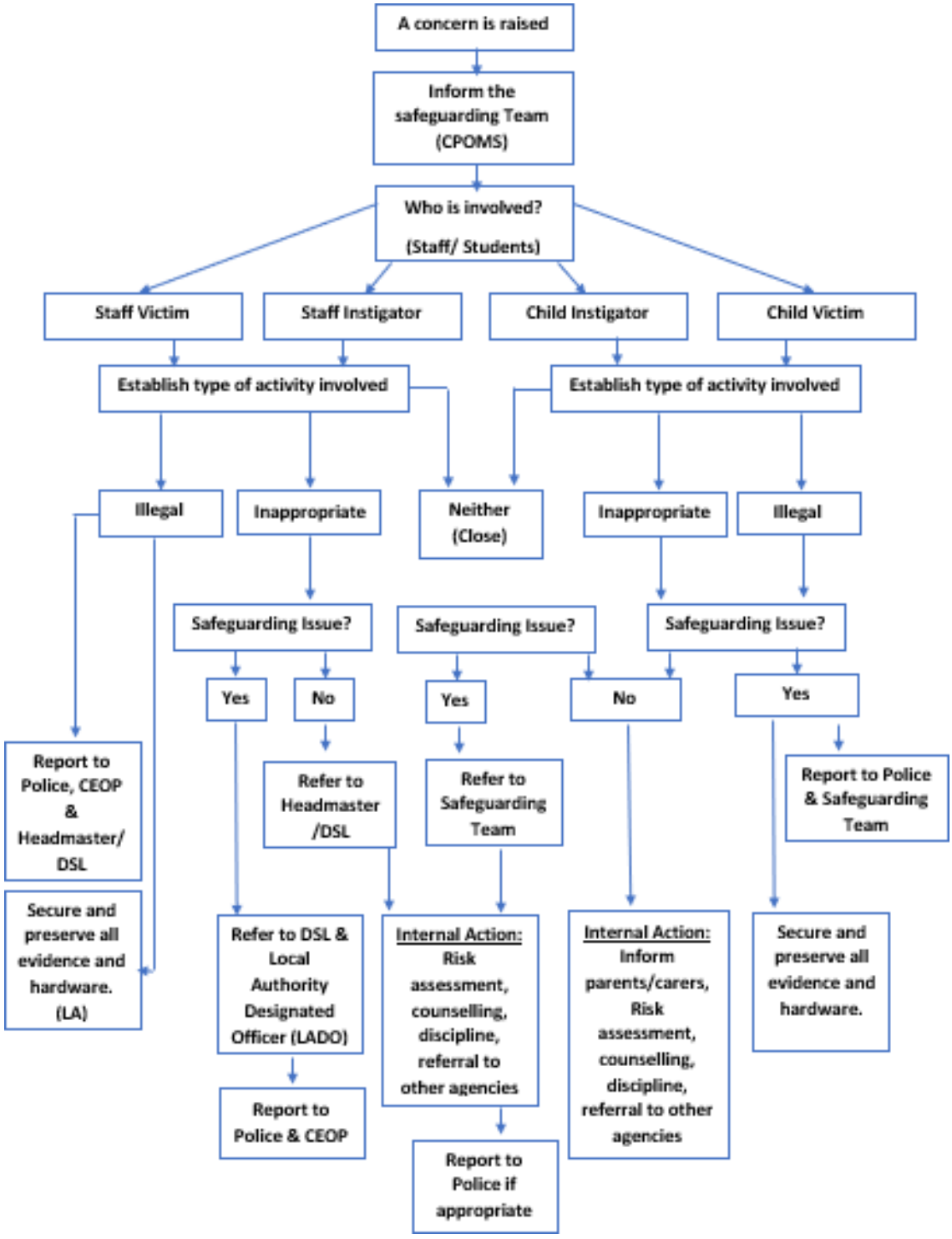
Staff should report the concern on CPOMs within 24 hrs. unless there is an imminent threat to the student's safety and wellbeing – in which case, you must stay with the student until a member of the Safeguarding Team can relieve you.

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 pupils.

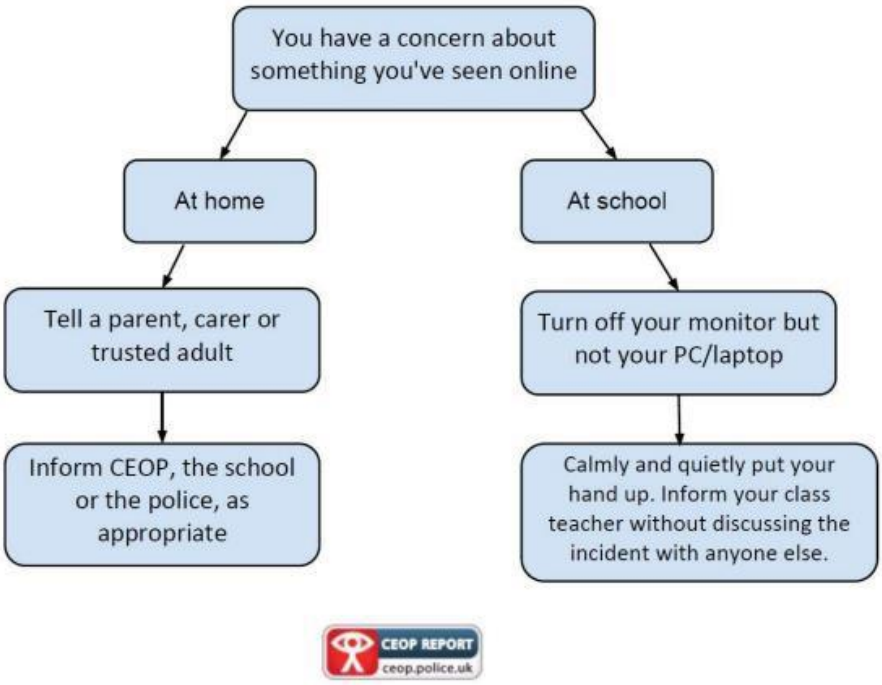
For more information on the reporting of a concern, please refer to the Safeguarding Policy or speak to a member of the Safeguarding Team.

***Pupils 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

Where the School provides remote or live online learning, the following expectations apply:

Staff

- All sessions must take place using approved school platforms (e.g. Microsoft Teams).
- Staff must ensure that sessions are secure, with access restricted to intended participants.
- Staff must maintain professional standards at all times, including dress, language, and environment.
- Staff should ensure that their background is appropriate and safeguarding-conscious.
- Attendance should be recorded at the start of each session.
- Staff must remain in control of the session environment, including the ability to mute or remove participants where necessary.
- Any safeguarding concerns must be recorded on CPOMS immediately.

Pupils

- Pupils must behave in line with school expectations and behaviour policies.
- Pupils should be in an appropriate setting suitable for learning, where possible.
- Pupils must use appropriate language and conduct.
- Pupils must not record, screenshot, or share content from live sessions.
- Pupils should only attend sessions for which they are authorised.

Use of Cameras and Audio

- The use of webcams and microphones should be guided by staff, taking into account:
    - Safeguarding
    - Privacy
    - Individual needs (including SEND and home circumstances)
- Pupils should not be required to use cameras where it would be inappropriate or cause distress.