The King's School
Canterbury

E-SAFETY POLICY

Person Responsible: Designated Safeguarding Lead
and the Safeguarding Team Member responsible for E-Safety

Date reviewed: March 2019

This policy will be reviewed annually or following any concerns and/or updates to national and local guidance or procedures.

The School recognises that Information Technology (IT) and the internet are fantastic tools for learning and communication that can be used in School to enhance the curriculum, challenge pupils, and support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in The School community, but it is important that the use of the internet and IT is seen as a responsibility and that pupils, staff and parents use it appropriately and practise good E-safety. It is important that all members of The School community are aware of the dangers of using the internet and how they should conduct themselves online.
E-safety education covers the internet, mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of The School community on the risks and responsibilities of E-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating IT activity in school, and provide a good understanding of appropriate IT use that members of The School community can use as a reference for their online conduct outside of School hours. E-Safety is a whole-School issue and responsibility.

Cyberbullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our Anti-Bullying Policy.

Communicating School policy

This policy is available to parents, staff, and pupils to access when and as they wish. Rules relating to The School code of conduct when online, and E-safety guidelines, are displayed around the school. E-Safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during Digital Curriculum and Life Matters lessons where personal safety, responsibility, and/or development are being discussed.

Contents

1. Policy Aims

- This E-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) 2018, and the Kent Safeguarding Children Board procedures.

- The purpose of the E-Safety policy is to:
  - Safeguard and protect all members of the School community online.
  - Identify approaches to educate and raise awareness of E-Safety throughout 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 E-Safety concerns.

- The School identifies that the issues classified within E-Safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- The School believes that E-Safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- The School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of The School(collectively referred to as 'staff' in this policy) as well as pupils and parents/Guardians.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with School issued devices for use off-site, such as work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
  - Anti-bullying policy
  - AUPs and codes of conduct
  - Behaviour and discipline policy
  - Child protection policy
  - Confidentiality policy
  - Curriculum policies, such as: Digital Curriculum (DC), Computer Science and Life Matters.
  - Data security
  - Image use policy
  - Mobile phone policy and social media, website and publication guidelines
  - Searching, screening and confiscation policy

3. Monitoring and Review

The School will review this policy at least annually. The policy will also be revised following any national or local policy requirements; any child protection concerns or any changes to the technical infrastructure.

- We will ensure that we regularly monitor internet use and evaluate E-Safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of E-Safety, the Headmaster will be informed of E-Safety concerns, as appropriate.
- The DSL will report to the named Governor for safeguarding on a regular basis on E-Safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The School has allocates a member of the DSL team to be in charge of E-Safety and this is reviewed whenever there is a change in the team.
- The School recognises that all members of the community have important roles and responsibilities to play with regards to E-Safety.

4.1 The SMT will:

- Ensure that E-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 E-Safety; including a codes of conduct and AUPs, which cover acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of School systems and networks.
- Ensure that E-Safety is embedded within a progressive whole School curriculum, which enables all pupils to develop an age-appropriate understanding of E-Safety.
- Support the DSL by ensuring they have sufficient time and resources to fulfil their E-Safety responsibilities.
- Ensure there are robust reporting channels for The School community to access regarding E-Safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate E-Safety practice to identify strengths and areas for improvement.

4.2 The DSL with responsibility for E-Safety will:

- Act as a 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 E-Safety and communicate this with The School community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate E-Safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that E-Safety is promoted to parents, Guardians and the wider community, through a variety of channels and approaches.
- Maintain records of E-Safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.

- Monitor E-Safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of E-Safety policies.
- Read and adhere to the E-Safety policy and AUPs.
- Take responsibility for the security of School systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed E-Safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of E-Safety issues and how they may be experienced by the children in their care.
- Identify E-Safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate E-Safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL, especially in the development and implementation of appropriate E-Safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the DSL.
- Report any filtering breaches to the DSL, as well as, the school's ISP or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

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

- Engage in age appropriate E-Safety education opportunities.
- Contribute to the development of E-Safety policies.
- Read and adhere to The School AUPs.
- 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 E-Safety issues.

4.6 It is the responsibility of parents and Guardians to:

- Read the School AUPs and encourage their children to adhere to them.
- Support the School in their E-Safety approaches by discussing E-Safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.

- Seek help and support from the School, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use School systems and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The School will establish and embed a progressive E-Safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including E-Safety in the DC, Life Matters and Computer Science programmes of study, plus house assemblies covering use both at School and home.
  - Reinforcing E-Safety messages whenever technology or the internet is in use.
  - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The School will support pupils to read and understand the AUP in a way which suits their age and ability by:
  - Displaying acceptable use posters in all rooms with internet access.
  - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Rewarding positive use of technology by pupils.
  - Implementing appropriate peer education approaches.
  - Providing E-Safety education and training as part of the transition programme across the key stages and when moving between establishments.
  - Seeking pupil voice when writing and developing School E-Safety policies and practices, including curriculum development and implementation.
  - Using support, such as external visitors, where appropriate, to complement and support the School's internal E-Safety education approaches.

5.1.1 Vulnerable Pupils

- 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 etc.

5.2 Training and engagement with staff

The School will:

- Provide and discuss the E-Safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate E-Safety training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that School systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing School systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding E-Safety concerns affecting pupils, colleagues or other members of The School community.

5.3 Awareness and engagement with parents and Guardians

- The School recognises that parents and Guardians have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The School will build a partnership approach to E-Safety with parents and Guardians by:
  - Providing information and guidance on E-Safety in a variety of formats. This will include offering specific E-Safety awareness training.
  - Drawing their attention to The School E-Safety policy and expectations in newsletters, letters, the prospectus and on the website.
  - Requesting that they read E-Safety information as part of joining school.
  - Requiring them to read The School AUP and discuss its implications with their children.

6. Reducing Online Risks

- The School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in School is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a School computer or device, but alerts to the DSL will be made whenever this occurs.
- All members of The School community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

Technology is used in School to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary IT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

- The School uses a wide range of technology. This includes, but is not limited to, access to:
  - Computers, laptops and other digital devices
  - The Internet which may include search engines and educational websites
  - School learning platform/intranet/VLE
  - Email
  - Digital cameras, web cams and video cameras

- All School owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place. (mobile device management software is in use and managed by IT. The IT steering committee agrees how access is recorded and enforced)
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The School will use age appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our community.
- The School will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age. The need to detect and prevent abuse, bullying or unsafe practice by children will be in accordance with the national minimum standards for boarding (NMS).

7.2 Managing Internet Access

- The School will maintain a record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an AUP before being given access to the School computer system, IT resources or internet.

7.3 Filtering and Monitoring

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found here.

7.3.1 Decision Making

- The School's governors and SMT have ensured that the School has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and SMT are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring takes into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by the appropriate staff with educational and technical experience with consent from the SMT; all changes to the filtering policy are logged and recorded.
- The DSL will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The School uses educational broadband connectivity through BT.
- The School uses IMPERO which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature via key word system which we have control over. The School filtering system blocks unsuitable sites (This should be reviewed via resources such as the Internet Watch Foundation (IWF) list).
- The School works with BT to ensure that our filtering policy is continually reviewed.
- The School has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff/ take screen shot.

  - The member of staff will report the concern (including the URL of the site if possible) to the DSL and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/Guardians will be informed of serious filtering breaches involving their child.
- Any material that The School believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

7.3.4 Monitoring

- The School will appropriately monitor internet use on all School owned or provided internet enabled devices.
- The School has a clear procedure for responding to concerns identified via monitoring approaches.
- All users will be informed that use of School systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998 and GDPR.
  - Full information can be found in the school's Data Protection Policy.

7.5 Security and Management of Information Systems

- The School takes appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on the school's network,
  - The appropriate use of user logins and passwords to access the School network.
- Specific user logins and passwords will be enforced for all users.
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security should be listed here.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access School systems; members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access School systems; pupils are responsible for keeping their password private.
- The School requires all users to:
  - Use strong passwords for access into our system.
  - Regularly change their passwords.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Never use the login of another.

7.6 Managing the Safety of The School Website

- The School will ensure that information posted on our website is up to date and meets current standards and requirements.

- The School will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the School addresses, emails and telephone numbers.
- The administrator account for the School website will be secured with an appropriately strong password.
- The School will post appropriate information about safeguarding, including E-Safety, on the School website for members of the community.

7.7 Publishing Images and Videos Online

- The School will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct, Social media and use of personal devices and mobile phones.

7.8 Managing Email

- Access to School email systems will always take place in accordance with Data protection legislation and in line with other School policies, including: confidentiality, AUPs and Code of conduct.
  - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the School community will immediately tell the DSL if they receive offensive communication, and this will be recorded in the School safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts *may* be blocked in school.
- The School has a dedicated email for reporting safeguarding and pastoral issues. These inboxes are managed by designated and trained staff.

7.8.1 Staff

- The use of personal email addresses by staff for any official School business is not permitted.
  - All members of staff are provided with a specific School email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

7.8.2 Pupils

- Pupils will use School provided email accounts for educational purposes and for any contact with School staff.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- The School recognises that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Videoconferencing contact details will not be posted publically.

- School videoconferencing equipment will not be taken off School premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents and Guardians consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the School will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The School will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

7.10 Management of Learning Platforms

- The School uses Firefly as its Virtual Learning Platform (VLE).
- SMT and staff will regularly monitor the usage of the VLE in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the VLE.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils and staff will be advised about acceptable conduct and use when using the VLE.
- All users will be mindful of copyright and will only upload appropriate content onto the VLE.
- Any concerns about content on the VLE will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the VLE for the user may be suspended.
  - The user will need to discuss the issues with a member of SMT before reinstatement.
  - A pupil's parent/guardian may be informed.
  - If the content is considered to be illegal, then the School will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

- A visitor may be invited onto the VLE by a member of the SMT only; in this instance, there may be an agreed focus or a limited time slot as deemed necessary.

7.11 Management of Applications (apps) used to Record Children's Progress

- The School uses a combination of ISAMs, SOCS and Firefly (and will soon introduce CPOMS) to track pupils progress and info share appropriate information with parents and Guardians via parent portal
- The Headmaster is ultimately responsible for the security of any data or images held of children. As such, via the DSL, he will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation
- In order to safeguard pupils' data:
  - Only School issued devices will be used for apps that record and store children's personal details, attainment or photographs.
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
  - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and Guardians will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of the School community.

- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
  - All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The School will control pupil and staff access to social media whilst using School provided devices and systems on site.
  - The use of social media during School hours for personal use is not permitted.
  - Inappropriate or excessive use of social media during school/work hours or whilst using School devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of the School community on social media, should be reported to the DSL and will be managed in accordance with our Anti-bullying, Whistleblowing against staff, Behaviour, Safeguarding and Child protection policies.

8.2 Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the School's code of conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within 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. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites as strictly as possible, and reviewing these 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 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 form 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 the SMT immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and 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 past pupils' family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this will be discussed with DSL and/or the Headmaster.
  - If ongoing contact with pupils 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, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headmaster.
- Any communication from pupils and parents received on personal social media accounts should be reported to the school's DSL.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The School is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing School policies including anti-bullying and behaviour. Concerns will also be raised

with parents/Guardians as appropriate, particularly when concerning underage use of social media sites or 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. Examples would include real/full name, address, mobile or landline phone numbers, School attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
  - 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/guardian 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 communications and report concerns both within School and externally.

8.4 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 him.
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the SMT.
  - SMT have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official School social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff must use School provided email addresses to register for and manage any official School social media channels.
  - Official social media sites are suitably protected.
  - Public communications on behalf of the School will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, guardians and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving pupils will be moderated by the School where possible.
- Parents and Guardians will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- 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.

Staff expectations

- Members of staff who follow and/or like the School social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

- 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 link
  - Be professional at all times and 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 being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace.
  - Ensure that 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 and guardians.
  - Inform their line manager, the DSL and/or the Headmaster of any concerns, such as criticism, inappropriate content or contact from pupils.

9. Use of Personal Devices and Mobile Phones

- The School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/guardians, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate School policies.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
  - All members of the School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the School accepts no responsibility for the loss, theft or damage of such items on School premises.
  - All members of the School community are advised to use passwords/PIN numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and PIN numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the School site according to the School mobile phone policy.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with the Behaviour policy.
- All members of the School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the School conduct or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant School policy and procedures.
- Staff are advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times and meetings.

  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods, unless in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phone numbers for contacting pupils or parents and guardians.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL and/or Headmaster.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
  - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
  - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the School policy, action will be taken in line with the School behaviour and Whistleblowing policies.
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- The School expects pupil's personal devices and mobile phones to be used according to the Mobile Phone policy.
- If a pupil needs to contact his/her parents or Guardians, they will be allowed to use a School phone if required.
- Mobile phones or personal devices will not be used by pupils during lessons or formal School time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
  - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
  - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the SMT.
- Mobile phones and personal devices must not be taken into examinations.
  - Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the School policy, the phone or device will be confiscated as per the Mobile Phone policy.
  - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy: www.gov.uk/government/publications/searching-screening-and-confiscation
  - Pupils' mobile phones or devices may be searched by a member of the SMT, with the consent of the pupil and/or a parent/guardian. Content may be deleted or requested to be deleted, if it contravenes School policies.
  - Mobile phones and devices that have been confiscated will be released according to School policy.
  - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

Parents, Guardians and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's AUP and other associated policies.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of School policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/guardians is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the AUP and mobile phone policy.

10. Responding to E-Safety Incidents and Concerns

- All members of the School community will be made aware of the reporting procedure for E-Safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official School procedures for reporting concerns.
  - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The School requires staff, parents, guardians and pupils to work in partnership to resolve E-Safety issues.
- After any investigations are completed the School will debrief and identify lessons learnt and implement any policy or curriculum changes as required.
- If the School is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place the School will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the School community for example, if other local schools are involved or the public may be at risk, the School will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupil Welfare

- The DSL will be informed of any E-Safety incidents involving safeguarding or child protection concerns.
  - The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that E-Safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- The School will inform parents and guardians of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the DSL or the Headmaster, according to the Whistleblowing policy.
- Any Whistleblowing regarding a member of staff's online conduct will be discussed by the DSL with the Local Authority Designated Officer (LADO).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

11. Procedures for Responding to Specific Incidents or Concerns

11.1 Youth Produced Sexual Imagery or "Sexting"

- The School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore, all concerns will be reported to and dealt with by the DSL.
- The School will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the KSCB guidance: "Responding to youth produced sexual imagery".
- The School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The School will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with 'Sexting'

- If the School is made aware of an incident involving the creation or distribution of youth produced sexual imagery, the School will
  - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
  - Immediately notify the DSL.
  - Store the device securely.

  If an indecent image has been taken or shared on the School network or devices, the School will take action to block access to all users and isolate the image:
  - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
  - Inform parents and guardians, if appropriate, about the incident and how it is being managed.
  - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
  - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
  - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Images will only be deleted once the School has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the SMT will also review and update any management procedures, where necessary.
- The School will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off School premises, using School or personal equipment.
- The School will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- ▪ In this case, the image will only be viewed by the DSL/DDSL and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.2 Online Child Sexual Abuse and Exploitation

- The School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- The School will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/guardians.
- The School will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The School will ensure that pupils are aware of the 'Click CEOP' report button.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- If the School is made aware of incident involving online sexual abuse of a child, the School will:
  - Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
  - Immediately notify the DSL.
  - Store any devices involved securely.
  - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/guardians about the incident and how it is being managed.
  - Make a referral to Specialist Children's Services (if required/ appropriate).
  - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; the SMT will review and update any management procedures, where necessary.
- The School will take action regarding online child sexual abuse, regardless of whether the incident took place on/off School premises, using School or personal equipment.
  - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report : www.ceop.police.uk/safety-centre/
- If the School is unclear whether a criminal offence has been committed, the DSL will take the necessary legal advice.
- If the School is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If pupils at other schools are believed to have been targeted, the School will seek support from Kent Police and/or CEOPs first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- The School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The School will take action regarding IIOC on School equipment and/or personal equipment, even if access took place off site.
- The School will take action to prevent accidental access to IIOC by using an ISP which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the School is unclear if a criminal offence has been committed, the DSL will take legal advice.
- If made aware of IIOC, the School will:

  - Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
  - Immediately notify the DSL.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, or that images of children have been found on School owned devices, or that a member of staff is in possession of indecent images of children, the DSL will:
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Ensure that the Headmaster is informed.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the school's managing Whistleblowing policy.
  - Quarantine any devices until police advice has been sought.
  - Report concerns, as appropriate to parents and guardians.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated.
- Full details of how the School will respond to cyberbullying are set out in the Anti-bullying policy.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at and will be responded to in line with existing School policies.
- All members of the community will be advised to report online hate in accordance with relevant School policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the School is unclear on how to respond, or whether a criminal offence has been committed, the DSL will seek legal advice.

11.6 Online Radicalisation and Extremism

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the School is concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately and action will be taken in line with the Safeguarding and Child protection policy.
- If the School is concerned that member of staff may be at risk of radicalisation online, the Headmaster will be informed immediately and action will be taken in line with the Child protection and Whistleblowing policies.

12. Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Ashley Assiter, e-Safety Development Officer esafetyofficer@kent.gov.uk Tel: 03000 415797

Guidance for Educational Settings:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
Kent e–Safety Blog: www.kentesafety.wordpress.com

THE SCHOOLB: www.The Schoolb.org.uk

Kent Police:

www.kent.police.uk or www.kent.police.uk/internetsafety
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

Kent Public Service Network (KPSN): www.kpsn.net
EIS - IT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

Action Fraud: www.actionfraud.police.uk
CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Professional E-Safety Helpline: www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools: www.360safe.org.uk