Kent College

Whole School e-Safety Policy (May 2018)

This policy has been written using the Kelsi Online Safety Guidance for Educational Settings It also takes into account the DfE statutory guidance “Keeping Children Safe in Education” 2018

Due to the constantly evolving nature of technology (including local and national guidance and legislation) this document will be updated frequently, making a note of the edition version used and checking Kelsi for updates.

Designated Safeguarding Lead: Louise Hallam

E-safety Officer: Jen Tobin

Named Governor with Leading Responsibility: Jane Stevens

Contents

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

Kent College believes that e-Safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

Kent College identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

As well as this, Kent College has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the school's management functions. The school also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

The purpose of Kent College's online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that the school is a safe and secure environment. Safeguard and protect all members of the school community online.
- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

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 girls and parents/carers.

This policy applies to all access to the internet and use of information communication devices including personal devices or where girls, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHCE), and Sex and Relationships Education (SRE).

Kent College identifies that the issues classified within online 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.

1.2 Key responsibilities of the community

1.2.1 Key responsibilities of the Senior Leadership Team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the E-Safety Officer in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect girls from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored. Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all girls to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an online safety culture.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Working with and support technical staff in monitoring the safety and security of schools' systems and networks.
- Ensuring a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Ensuring that the Designated Safeguarding Lead (DSL) works in partnership with the E-Safety Officer.

1.2.2 Key responsibilities of the E-Safety Officer are:

- Working in partnership with the DSL and Safeguarding team.
- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the school for data protection and data security and to ensure that practice is in line with legislation.
- Ensuring that online safety incidents and actions taken are recorded during pastoral and Safeguarding meetings

Monitoring such incidents and identify gaps/trends to respond to. Reporting this back to the school leadership team, Governing Body and other agencies as appropriate.

- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

12.3 Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of the school's systems and data through individual use.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.

Identifying individuals of concern, and reporting these to the E-Safety Officer or relevant Head of School.

- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

1.2.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- Ensure that suitable access controls and encryption are implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the E-Safety Officer and DSL.

- Ensuring that the use of the setting’s network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E-Safety Officer and DSL.
- Reporting any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded within the Safeguarding minutes, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Reportingany breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the E-Safety Officer and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school’s ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensuring that appropriately strong passwords are applied and enforced for all but the youngest users.

1.2.5 Key responsibilities of girls are:

- Contributing to the development of online safety policies.
- Reading and signing the Pupil Acceptable Use Policy and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.2.6. Key responsibilities of parents and carers are:

- Reading the Pupil Acceptable Use Policy, encouraging their daughter to adhere to it, and adhering to it themselves where appropriate.
- Discussing online safety issues with their girls, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their daughter is at risk of harm online and communicating this to the school.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school's online safety policies.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.

- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Headmistress will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)

Pupils work will only be published with their permission or that of their parents/carers.

The administrator account for the school website will be safeguarded with an appropriately strong password.

The school will post information about safeguarding, including online safety on the school website.

2.2 Publishing images and videos online

The school will ensure that all images are used in accordance with the schools' Taking, Storing and Use of ImagesPolicy

2.3 Managing email

Pupils may only use their school provided email accounts for educational purposes.

All members of staff are provided with a specific school email address to use for any official communication.

The use of personal email addresses by staff for any official school/setting business is not permitted.

The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.

Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.

Sensitive or personal information will only be shared via email in accordance with data protection legislation.

Whole -class or group email addresses may be used for communication outside of the school (in early years, infant and primary schools).

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted.

Email sent to external organisations and parents should be written carefully and checked (where appropriate) by a line manager before sending, in the same way as a letter written on school headed paper would be.

The reporting of wellbeing and pastoral issues should be emailed to Form Tutors, in the first instance, and copied to the girl's Head of School. Alternatively there is the help@ email address which girls can contact with any concerns..
School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.3.1 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. (

2.3.2 Girls

  - Girls will use school provided email accounts for educational purposes.
  - Girls will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
  - Whole-class or group email addresses may be used for communication outside of the school (in early years, prep school).

2.4 Appropriate and safe classroom use of the internet and associated devices

- Kent College uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - School learning platform/intranet
  - Email
  - Games consoles and other games based technologies
  - 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.
- 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 such as SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search, following an informed risk assessment, to identify which tool best suits the needs of the community.
- The school will ensure that the use of internet-derived materials, by staff andgirls, complies with copyright law and acknowledge the source of information.
- Supervision of girls will be appropriate to their age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Girls' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for their age and ability.
  - **Key Stage 2**
    - Girls will use age-appropriate search engines and online tools.
    - Girls will be directed by the teacher to online materials and resources which support the learning outcomes planned for their age and ability.

- **Key Stage 3, 4, 5**
  - Girls will be appropriately supervised when using technology, according to their ability and understanding.
  - **Boarders**The school will balance a girl's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

2.5 Educational use of Videoconferencing and/or Webcams

Kent College recognise 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.
- Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
- 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.

2.5.1 Users

- Parents and carers 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, according to the pupils' age and ability. (schools should list how this will be enforced and achieved)
- Video conferencing 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.

2.5.2 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.

2.6 Management of Learning Platforms

Kent College uses Firefly as its official learning platform.

Staff will regularly monitor the usage of the Learning Platform (LP) 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 LP.
- 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.
- Girls and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP 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 LP for the user may be suspended.
  - The user will need to discuss the issues with a member of senior leadership team before reinstatement. A girl's parent/carer may be informed.
  - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
  - Girls may require editorial approval from a member of staff. This may be given to the girl to fulfil a specific aim and may have a limited time frame.
  - A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

2.7 Management of Applications (apps) used to Record Girls' Progress

- Teachers may use apps such as Tapestry to track pupils' progress and share appropriate information with parents and carers.
- The Headmistress is ultimately responsible for the security of any data or images held of children. As such, she 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.
  - In line with GDPR and the school's AUP, staff's personal mobile phones or devices will not be used to access or upload content to any unsecure apps which record and store children's personal details, attainment or images. Any educational apps used 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 carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

3.Social Media Policy

3.1. General social media use

Expectations regarding safe and responsible use of social media will apply to all members of the Kent College community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of the school community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community.
- 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 (either in a public or a private setting), especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupils and staff access to social media and social networking sites whilst on site and using school provided devices and systems.
- Inappropriate or excessive use of social media, including impersonation of others, either during school hours, whilst using school devices or when concerning other members of the school community may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the E-Safety Officer or DSL and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Official use of social media

Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.

Official use of social media sites as communication tools will be risk assessed and formally approved by the Headmistress.

Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.

Staff will use school provided email addresses to register for and manage official school approved social media channels.

Members of staff running official school social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.

All communication on official school social media platforms will be clear, transparent and open to scrutiny.

Any online publication on official school social media sites will comply with legal requirements including the Data Protection Act 1998, GDPR 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

Official social media use by the school will be in line with existing policies including anti-bullying and child protection.

Images or videos of girls will only be shared on official school social media sites/channels in accordance with the school image use policy.

Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.

Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Senior Leadership Team.

Parents/Carers and pupils will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.

Kent College's official social media channels are:

- Twitter
- Facebook)
- YouTube
- GooglePlus
- Instgram
- LinkedIn

Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.

The school social media account will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.

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.

3.3 Staff official use of social media

If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and that they are an ambassador for the school.

Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.

Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.

Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.

Staff must ensure that any image posted on the school social media channel have appropriate written parental consent.

Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

Staff using social media officially will inform their line manager, the E-Safety Officer or the Headmistress of any concerns such as criticism or inappropriate content posted online.

Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and should communicate via school communication channels.

Staff using social media officially will sign the school social media Acceptable Use Policy before official social media use will take place.

3.4 Staff personal use of social media

Personal 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 Acceptable Use Policy.

No members of staff are to communicate with or add as 'friends' any current pupils or current 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 the E-Safety Officer or Headmistress.

If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.

Staff are advised to avoid 'friending' former pupils, but where this does occur the former pupil should be over 18 and have been off the school role for a minimum of 2 years.

All communication between staff and members of the school community on school business will take place via official approved communication channels (*such as school email address or phone numbers*). Staff must not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headmistress.

Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead and will be logged.

Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with the school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.

Members of staff are encouraged not to identify themselves as employees of Kent College on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.

Members of staff will ensure that they do not represent their personal views as that of the school on social media.

School email addresses will not be used for setting up personal social media accounts.

Members of staff who follow/like the school's social media channels will be advised to use dedicated professional accounts where possible to avoid blurring professional boundaries.

3.5 Girls use of social media

Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school Acceptable Use Policy.

Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding 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/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones for girls

Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
Mobile phones and personal devices are not permitted to be used at certain times within the school.

- Prep School – No mobile phones in school
- Senior School (Year 7-10) – No mobile phones permitted in school during the school day. All phones are handed into tutors at the start of the school day (8:30am) and stored in a secure office until the end of the school day (4pm) where they can then be collected.
- Senior School (Year 11 and Sixth Form) – Mobile phones should not be used around the school site or in the Dining Hall. Year 11 and Sixth Formers can use their mobile phones in designated open access areas such as form rooms, the Year 11 Common Room and Tilley, but must not use them in areas used for shared study (LRC) or in lessons.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
Members of staff will be issued with a school/work phone number and email address where contact with pupils or parents/carers is required.
All members of the school community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
All members of the school community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
All members of the school community will be 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 policies.
School mobile phones and devices must always be used in accordance with the Acceptable Use Policy
School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Girls use of personal devices and mobile phones

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, then it will only take place when approved by the Senior Leadership Team.

If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the pupil's Head of School, Deputy Head Pastoral or Headmistress.

Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Phones and 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, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school 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. The phone or device may be searched by a member of the Senior Leadership Team with the consent of the pupil or parent/carer.

Searches of mobile phone or personal devices will be carried out in accordance with the school's policy Acceptable Use Policies and Bullying 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, then the device will be handed over to the police for further investigation.

4.3.1 Concerns about Girls Welfare

- The DSL will be informed of any online 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 online 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 carers of any incidents or concerns involving their child, as and when required.

4.3.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headmistress, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the DSL, Deputy Head Pastoral, Headmistress and in some cases the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of Conduct.

4.4 Staff use of personal devices and mobile phones

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with the Senior Leadership Team.

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times or left in a secure office/workroom.

Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.

Personal mobile phones will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances.

Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.

If a member of staff breaches the school policy, then disciplinary action will be taken.

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, then the police will be contacted and allegations will be responding to following the allegations management policy.

4.5 Visitors use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

Kent College is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

Emerging technologies will be examined for educational benefit and the Senior Leadership Team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.

The school will audit technology use to establish if thee-Safety policy is adequate and that the implementation of the policy is appropriate.

Methods to identify, assess and minimise online risks will be reviewed regularly by the SafeguardingTeam and Senior Leadership.

Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the Senior Leadership Team.

5.2. Internet use within the community

The school will liaise with local organisations to establish a common approach to e-Safety.

The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

5.3 Authorising internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school ICT resources.

Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of girls

An online e-Safety curriculum will be established and embedded throughout the whole school, particularly in the PSHE, RSE and ICT programmes of study covering both safe school and home use.
Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
All users will be informed that network and Internet use will be monitored.
The Pupil Acceptable Use expectations and posters will be posted in all rooms with Internet access.

6.2 Engagement and education of girls who are considered to be vulnerable

Kent College is aware that some girls are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
Kent College will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
Kent College will seek input from specialist staff as appropriate, including the SENCO, Heads of School, DSL and Deputy Head Pastoral.

6.3 Engagement and training of staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. (Either as stand-alone training or as part of the annual Child Protection training). 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 online safety concerns affecting pupils, colleagues or other members of the school community.

6.4 Engagement and education of parents and carers

Kent College recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

Parents' attention will be drawn to the school's e-Safety policy and expectations in newsletters, lettersand on the school website.

A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events and sports days.

Parents will be requested to read online safety information as part of the Home School Agreement.

Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

Information and guidance for parents on online safety will be made available to parents in a variety of formats.

Parents will be encouraged to role model positive behaviour for their children online.

7. Managing Information Systems

7.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Full information regarding the schools approach to data protection and information governance can be found in the school's Privacy Policy

7.2 Security and Management of Information Systems

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.

Portable media may not be used without specific permission followed by an anti-virus /malware scan.

Unapproved software will not be allowed in work areas or attached to email.

Files held on the school's network will be regularly checked.

IT Network Manager will review system capacity regularly.

The appropriate use of user logins and passwords to access the school network will be enforced for all but the youngest users.

All users will be expected to log off or lock their screens/devices if systems are unattended.

The school will log and record internet use on all school owned devices via the IT department's Securus program.

7.2.1 Password Policy

All users will be informed not to share passwords or information with others and not to login as another user at any time.

Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.

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 (excluding nursery and early years) are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.

We require staff and pupils to use strong passwords for access into our system.

We require staff and pupils to change their passwords every 6 months.

7.3 Filtering Decisions

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

The school uses Lightspeed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.

The school uses Securus alongside Lightspeed to monitor activity within the network.

The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.

The school will work with CTS to ensure that filtering policy is continually reviewed.

The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.

If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.

The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

All changes to the school filtering policy will be logged and recorded.

The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.

Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP immediately.

7.3.1 Dealing with Filtering Breaches

- 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.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of 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.

8. Responding to Online Incidents and Concerns

All members of the school/setting community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

The Designated Safeguarding Lead (DSL) will be informed of any e-Safety incidents involving child protection concerns, which will then be recorded.

The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure.

Any complaint about staff misuse will be referred to the Headmistress.

Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Pupils, parents and staff will be informed of the school's complaints procedure.

Staff will be informed of the complaints and whistleblowing procedure during their induction.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

The school will manage e-Safety incidents in accordance with the school discipline/behaviour policy where appropriate.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or Kent Police via 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.

If the school is unsure of how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent.

Parents and children will need to work in partnership with the school to resolve issues.

Agreed: Exec May 2018

Approved by Education Committee: June 2018

Updated: ESafety Officer: October 2018

Approved by Education Committee: November 2018

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions reading online safety concerns and has been written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventuality so professional judgement and support from appropriate agencies such as the Education Safeguarding Team, Police, CSET and Children's Social Care is encouraged.

Some settings may not feel that these sections are relevant due to the age and ability of children; however, it is recommended that designated safeguarding leads ensure that their settings safeguarding policies and procedures are robust and are applicable for a range of safeguarding issues should they occur.

Some schools and settings will place these sections within existing safeguarding and child protection policies and procedures rather than the online safety policy or within other appropriate policies and procedures. Other settings will prefer to keep this content as reference material for Designated Safeguarding Leads.

9.1 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

Kent College ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").
The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
Kent College views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (*Louise Hallam Assistant Head*).
If the school are made aware of incidents involving indecent images of a child, 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 designated safeguarding lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.

- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

The school will not view the image unless there is a clear need or reason to do so.

The school will not send, share or save indecent images of children and will not allow or request children to do so.

If an indecent image has been taken or shared on the school/settings network or devices, then the school will take action to block access to all users and isolate the image.

The school will need to involve or consult the police if images are considered to be illegal.

The school will take action regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it" and a Briefing Note – "Police Action in Response to Youth Produced Sexual Imagery (Sexting)." Published by the College of Policing.

The school will ensure that all members of the community are aware of sources of support.

9.2. Responding to concerns regarding Online Child Sexual Abuse

Kent College will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

Kent College views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (*Louise Hallam Assistant Head*).

If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the school are made aware of incident involving online child sexual abuse of a child, then 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 designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform Kent police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.

- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
If pupils at other schools are believed to have been targeted, then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

Kent College will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the school/setting are made aware of Indecent Images of Children (IIOC) then the school will:

- Act in accordance with the schools' child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
- Immediately notify the school Designated Safeguard Lead.
- Store any devices involved securely.
- Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- 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.

If the school are made aware that indecent images of children have been found on the schools' electronic devices, then the school will:

- Ensure that the Designated Safeguard Lead is informed.
- 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.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:

- Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation or extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. The School will need to highlight specifically how internet use will be monitored either here or within subsequent sections. When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

9.5. *Responding to concerns regarding cyberbullying*

Cyberbullying, along with all other forms of bullying, of any member of the Kent College community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded. This includes accusations against a member of the Kent College Community from external agencies.

There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.

Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.

- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

9.6 Online Hate

- Online hate content directed towards, or posted by, specific members of the community will not be tolerated at Kent College and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- 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 Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

Appendix C
e-SafetyContacts and References

Kent Support and Guidance

- Claire Ray Principal Officer 03000 415788 07920 108828 claire.ray@theeducationpeople.org
- Peter Lewer Training & Development Officer 03000 418707 07740 183807 peter.lewer@theeducationpeople.org
- Linda Funnell Education Safeguarding Support Officer 03000 411995 linda.funnell@theeducationpeople.org
- Rebecca Avery Education Safeguarding Adviser – Online Protection
- Ashley Assiter e-Safety Development Officer (Maternity leave till January 2019)
- Kay Ashman Admin Support 03000 415797 07789 968705 07545 743310
- General enquiries: esafetyofficer@theeducationpeople.org

- 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

KSCB:

- www.kscb.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:

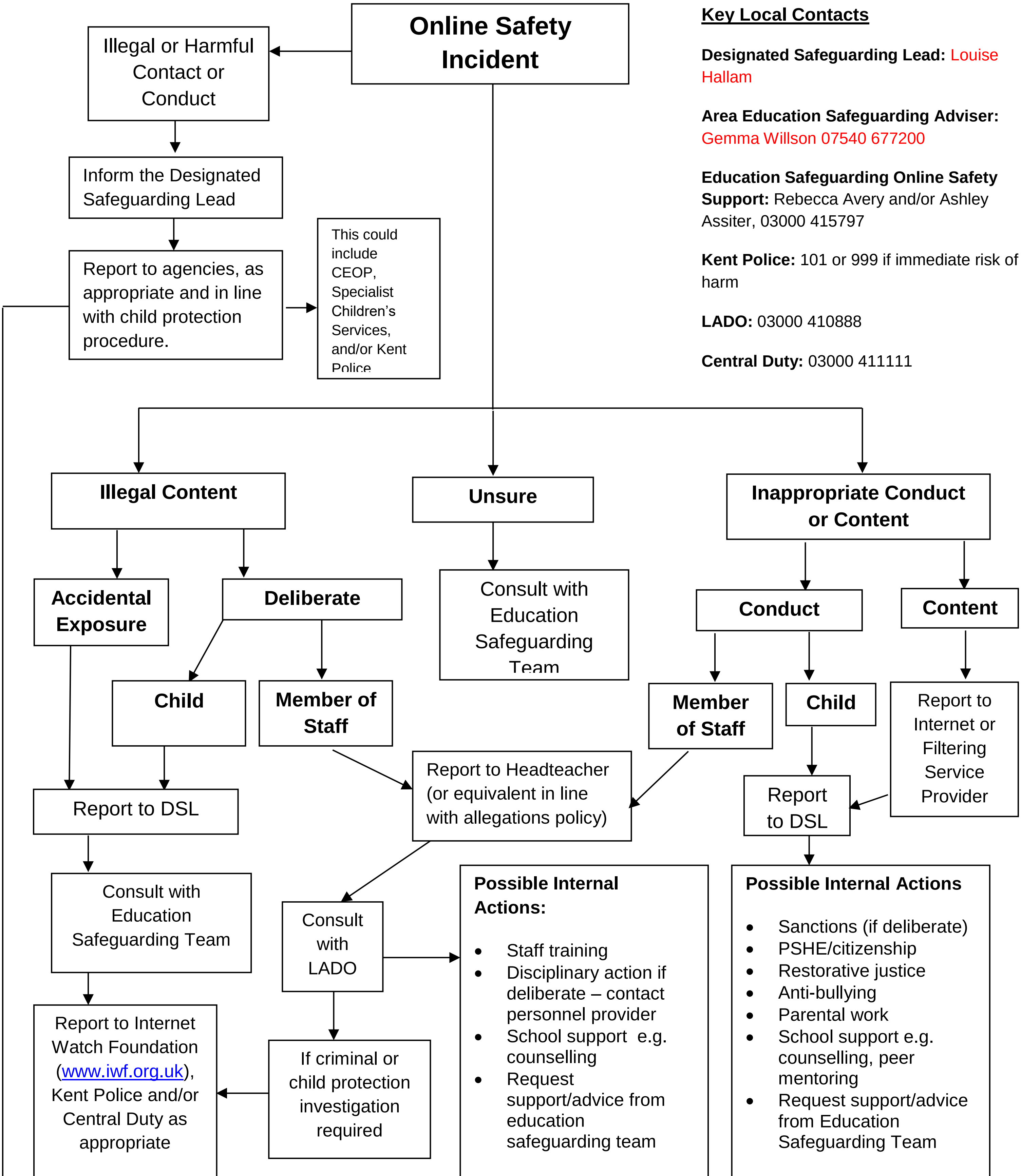
- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

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 Online Safety Helpline: www.saferinternet.org.uk/about/helpline

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

Appendix D: Responding to an Online Safety Concern


Online Safety Incident
Illegal or Harmful Contact or Conduct
Inform the Designated Safeguarding Lead
Report to agencies, as appropriate and in line with child protection procedure.
This could include CEOP, Specialist Children's Services, and/or Kent Police
Illegal Content
Unsure
Inappropriate Conduct or Content
Accidental Exposure
Deliberate
Consult with Education Safeguarding Team
Conduct
Content
Child
Member of Staff
Member of Staff
Child
Report to Internet or Filtering Service Provider
Report to Headteacher (or equivalent in line with allegations policy)
Report to DSL
Report to DSL
Consult with Education Safeguarding Team
Consult with LADO
Possible Internal Actions:
Staff training
Disciplinary action if deliberate – contact personnel provider
School support e.g. counselling
Request support/advice from education safeguarding team
Possible Internal Actions
Sanctions (if deliberate)
PSHE/citizenship
Restorative justice
Anti-bullying
Parental work
School support e.g. counselling, peer mentoring
Request support/advice from Education Safeguarding Team
Report to Internet Watch Foundation (www.iwf.org.uk), Kent Police and/or Central Duty as appropriate
If criminal or child protection investigation required

Key Local Contacts

Designated Safeguarding Lead: Louise Hallam

Area Education Safeguarding Adviser: Gemma Willson 07540 677200

Education Safeguarding Online Safety Support: Rebecca Avery and/or Ashley Assiter, 03000 415797

Kent Police: 101 or 999 if immediate risk of harm

LADO: 03000 410888

Central Duty: 03000 411111