KENT COLLEGE
CANTERBURY

# Kent College Online Safety Policy

| | |
|---|---|
| **Owner** | Designated Safeguarding Lead, Senior School & Designated Safeguarding Lead, Junior School |
| **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 children and parents/carers on school premises or away from the school on an activity, visit or other educational pursuit |
| **Date last reviewed** | September 2021 |
| **Date of next review** | September 2023 |
| **Review period** | 2 years |

## Introduction

It is the duty of Kent College to ensure that every pupil in its care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include: Websites; Email and instant messaging; Blogs; Social networking sites; Chat rooms; Music / video downloads; Gaming sites; Text messaging and picture messaging; Video calls; Podcasting; Online communities via games consoles; and Mobile internet devices such as smart phones and tablets.

This policy, supported by the separate Acceptable Use Policies for all staff and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

It is linked to the following school policies: Safeguarding; Staff Code of Conduct; Health and Safety at Work; Behaviour Policy and Practice; Anti-Bullying; Acceptable Use Policies; Data Protection Policy.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks

associated with the use of these internet technologies.

At Kent College, we understand the responsibility to educate our pupils on Online Safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about Online Safety and listening to their fears and anxieties as well as their thoughts and ideas.

**Scope of this Policy**

This policy applies to all members of the school community, including staff, pupils, parents and visitors who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and legal or educational guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the separate Acceptable Use Policies for all staff and pupils cover both fixed and mobile internet devices provided by the school (such as macbooks, PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc) as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smartphones, etc.).

This policy has been prepared following consultation and discussion with stakeholders including but not limited to teaching and in class support staff, governors, houseparents, IT technical support staff, parents and pupils, and referring to the guidance from ISBA and KELSI.

**Roles and responsibilities**

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually. The nominated member of the Governing Body for Safeguarding and Online Safety, Mrs Georgina Baker, or her deputy, Mrs Jean Gray, will liaise with the Designated Safeguarding Leads on a regular basis. Mrs Baker and Mrs Gray are suitably trained in safeguarding and promotion of welfare.

2. The Head and the Senior Leadership Team

The Head has overall responsibility, with the Head of Junior School each being responsible for the safety of the members of the Junior school communities and this includes responsibility for Online Safety. The Head of Junior School has delegated day-to-day responsibility to the Designated Safeguarding Leads for the Junior School respectively.

In particular, the role of the Headmaster senior school and Junior School Headmaster and the Senior Leadership team is to ensure that: staff, in particular the Designated Safeguarding Leads are adequately trained about Online Safety and staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of Online Safety in connection to the school.

3. Online Safety Coordinator

The School's Designated Safeguarding Lead in the Senior School, Mr Dan Bennet and in the Junior School, Mrs Zen Stedman is the respective school's Online Safety Coordinator and is responsible to the respective Heads' for the day to day issues relating to Online Safety. The Online Safety Coordinator has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current Online Safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Kent Safeguarding Children Multi-agency Partnership.

4. IT staff

The school's technical staff have a key role in maintaining an ethical and safe technical infrastructure at the school and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the school's hardware systems, its data and for induction/training the school's teaching and administrative staff in the use of IT. They have oversight of internet use and email although emails are not routinely monitored. IT staff maintain content filters, and will report inappropriate usage to the Online Safety Coordinator, a daily digest of which goes to the Director of ICT and the DSL.

5. Teaching and Support staff

All staff are required to sign the Staff Acceptable Use Policy before accessing the school's systems after induction. Staff may also be asked to update their understanding and sign subsequent issues of the AUP.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any Online Safety issues which may arise in classrooms or around the school on a daily basis.

Staff should not encourage nor facilitate any online activity that is intrinsically unsafe or exposes pupils or other members of staff to danger or significant risk. It is the responsibility of those responsible in the classroom to monitor the online activities of the pupils through normal good classroom practice such as, for example, circulating around the classroom and talking to the pupils, or positioning themselves such that the teacher can see all the screens, and to assess the risk of any online learning activity set by them.

The school Google Classroom and Google Chat facilities provide secure, closed social media and instant messaging platforms for educational purposes within the classroom boarding or school trips, and it is expected that these are the default platforms for use when communicating with pupils or about pupils. Purely educational resource curation platforms such as Scoop.it are acceptable but teachers must be mindful of their responsibility to check the suitability of any resource curated on the site. These should follow the expectations outlined in the staff code of conduct, Online Safety Policy and Staff AUP, be for school related matters only, conducted in a professional manner, and should be closed or deleted as soon as the activity or trip is completed. The default is that a school account or school device should be used for such communications but, in the unlikely event that a personal mobile device was needed to be used due to an emergency, as soon as possible the communication should be transferred to a school device. If there is a need for a longer use of a personal

device, then advice should be sought from the Online Safety Coordinator or the Trips Coordinator.

Staff are allowed to operate social media sites wholly administered for public facing marketing and publicity purposes under the direction of and with full knowledge of the Senior Management Team of Kent College but must be used with caution and moderated regularly. Personal information regarding children must be limited to their first names only, and staff should be mindful of any restrictions on individual children being photographed or named at all.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy (Senior School) or the Online Safety Pledge (Junior School), and for letting staff know if they see IT systems being misused.

7. Parents

Kent College believes that it is essential for parents to be fully involved with promoting Online Safety both in and outside of school. We regularly consult and discuss Online Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Pupil Acceptable Use Policy.

**Education and training**

1. Staff: awareness and training

New staff receive information on Kent College's Online Safety and Staff Acceptable Use policies as part of their induction.

All staff receive periodic information updates and, at least annually, training on Online Safety issues in the form of INSET training and/or internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety.

Agencies for supply teaching staff provide details of training and checks and supply teaching staff receive a briefing sheet on their first day of work that includes guidance about Online Safety. Long term agency staff receive full safeguarding training including online safety.

Contractors receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Visitors to the school receive information about Online Safety within the visitors' Safeguarding leaflet issued at the point of signing in.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. These

behaviours are summarised in the Pupil Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT policies and applicable legislation.

Teaching staff are encouraged to incorporate Online Safety activities and awareness within their subject areas and adopt a culture of talking about issues as they arise.

Staff should know what to do in the event of misuse of technology by any member of the school community. If Staff have any concerns or if any incident relating to Online Safety occurs, they should report them as soon as possible directly to the school's Designated Safeguarding Lead.

2. Pupils: Online Safety and Safeguarding in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for Online Safety and safeguarding guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote Online Safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about Online Safety and safeguarding within a range of curriculum areas and specifically in IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school may also be carried out via PSHE and by, for example, presentations in chapel, as well as informally when opportunities arise, such as discussions in tutor groups.

At age-appropriate levels, and usually via PSHE and ICT, pupils are taught about their Online Safety responsibilities and how to look after their own Online Safety and safeguarding. From Year 8, pupils are formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Designated Safeguarding Lead and any member of staff at the school.

From Year 7 onwards, pupils are also taught about relevant laws applicable to using the internet; such as computer misuse, data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils are also taught about the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead, the School Counsellor, as well as parents, house parents, peers, the IT helpdesk and other school staff for advice or help if they experience problems when using the internet and related technologies.

The following aspects of Online Safety are examples of what Online safety topics are covered within the curriculum:

Early Years Foundation Stage: The internet is not used by the children within EYFS but teachers will discuss Online Safety if it comes up in conversation and conduct any searches for the children as a learning activity.

In Early Years and Key Stage 1 the children are taught about how to access information and what to do if something they aren't sure of appears on screen. They are also taught not to answer online questions or give any personal information out at all.

Juniors develop this knowledge and also cover specific internet safety touching on using social media. What is appropriate to share, what we should do if something unpleasant happens on screen or is sent directly to us. How to deal with specific concerns a child may have. This is taught in specific lessons and is discussed regularly in ICT sessions so that all children are aware of how to utilise devices safely both at home and in school and how to tackle any problems or concerns they may have.

Examples of what can be taught:

Year 7: ICT Cyberbullying: What is cyberbullying? How to avoid being a bystander or accessory. How to deal with cyberbullying. PSHE Personal development, Relationships, communications (including electronic), boundaries. Values, decisions, bullying (including Online Safety), Puberty.

Year 8: ICT Search Engines: How to search the internet safely. How to recognise appropriate websites. How reliable is online information? Safe Passwords. Social Networking. How to use social networking safely. What not to do. Online grooming. PSHE Risk (risky situations), managing emotions, trust & assertiveness; moral codes. Bullying revisited (Online Safety and risk.)

Year 9: ICT: Looking after personal information online. Your digital footprint. How to protect yourself online. Using a mobile phone safely. Email, antivirus and firewalls. PSHE: Personal responsibility, risky situations, managing impulses, assertiveness, personal change, Sex and Relationships Education.

Year 10 PSHE: Personal Responsibility: Managing emotions & risk, trust and assertiveness, moral codes, bullying.

Year 12 and 13 Induction and Key Skills: Safeguarding and Online Safety

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of Online Safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges annual discussion evenings for parents and advises about Online Safety and also on the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. All parents receive electronic links to Digital Parenting and a paper copy is also mailed where possible.

**Policy Statements**

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a unique password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access. Some staff may have devices which have encryption to protect data stored on them.

Staff are permitted to bring in personal devices such for their own use only and are expected to use them within professional bounds and keeping to the Staff Acceptable Use Policy.

Personal telephone numbers, email addresses, or other contact details should not normally be shared with pupils or parents; if it is necessary to do so, any pupil or parental contact details should be removed from personal phone or email directories as soon as possible.

Pupils

**Junior School**

Children in Years 5 and 6 may bring a mobile phone to school by arrangement (for example if they are taking the bus to and from school.) These are handed in to the school office upon arrival and are collected upon departure.

Beginning In Year 1, where appropriate, children receive a student log-in which enables them to access Google suite without email.

**Senior School**

Some Pupils are allowed to bring mobile phones to school. According to the rules within the Kent College Handbook and our Mobile Phone Policy years 7-9 are not. This applies to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school provides technologies for pupil use. Macbooks are provided to all pupils in the Senior School and an IT suite and iPADS and Chomebooks are available for use at the Junior School.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with The SENDCO to agree how the school can appropriately support such use. The SENDCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of Internet and email

Staff

Staff are expected to maintain professional conduct when accessing personal email or any personal website at all times, be this on a school provided computer or their own device. Staff should use social networking sites with extreme caution, being aware of the nature of what is

published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff who need one are issued with their own school email address for work purposes for use on our network and by remote access. Teaching staff are also issued with a Canterburians email address for communicating directly with pupils about curriculum matters and for use on google classroom. Access is via a personal login, which is password protected and all work email communications should be conducted through this. Staff should be aware that email communication sent from the school email systems is bound to a school owned domain name and as such all communications represent the school. Staff should represent only the most positive views when communicating with parents, suppliers and other agencies outside of the school domain

Staff should note that email, some elements of social network traffic and instant messaging may be virus scanned, subject to an acceptable word list and should only be used for bona fide school business. A pre-formed disclaimer may be added to each email without explicit permission of the staff member.

Personal email should therefore be sent through one of the many web-mail services such as Gmail or Hotmail mail servers rather than the school email account. It is recommended that this kind of activity is kept on personally owned devices such as smartphones and tablets etc.

Social Networks

Staff are expected to use social networks responsibly and to consider the ramifications of posting messages from school premises and computers or to online groups with memberships of current students or parents. As a default a separate social network from the member of staff's school account and identity should be used for school purposes. **Pupils should not be exposed to contact with other non- Kent College authorised adults across school related social networks nor with staff using their personal email or social network accounts.** Pictures of staff and pupils published on the web should be in line with the school's policy on use of pupil images and staff should be mindful of misinterpretation or manipulation of such images when placed on the WWW.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and they must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT technical team.

Any online communications must not either knowingly or recklessly: place a child or young person at risk of harm, or cause actual harm; breach confidentiality; breach copyright; breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by: making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age; using social media to bully another individual; or posting links to or endorsing material which is discriminatory or offensive or bring Kent College into disrepute.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances should staff contact, on school business, a pupil or parent/carer using any personal email address. The school ensures that staff have access to

their work email address when offsite, for use as necessary on school business.

Governors

Additionally, governors are specifically provided with their own personal school based email address separate to the main school system but bound to a school owned domain and have their own separate area where documents are stored and available to access online. This enables them to conduct all official governor business associated with the school securely via the school email system and not on a personal email address.

Pupils

All senior school pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work assignments / research / projects. Pupils should be aware that email communications go through the school network and although school email addresses are not routinely monitored they may be subject to viewing and are therefore not necessarily private.

There is strong antivirus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the IT technical team for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the Online Safety Coordinator/IT technical team/or another member of pastoral staff.

The school expects pupils to think carefully before they post any information online, or re-post or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of an inappropriate or distressing nature directly to the DSL/ or another member of pastoral staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the school's Pupil Acceptable Use Policy and the Behaviour - Policy and Practice. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the IT technical team for assistance.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policies for further details.

Staff and pupils are expected to normally save all data relating to their work to their school macbook or to their Google Drive Account or an iCloud account. Any portable storage media should be encrypted or password protected. The IT technical team can be consulted for

advice in this respect.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Online Safety Coordinator or the IT technical team.

4. Password security

Pupils and staff have individual school network logins and email addresses and storage on the cloud. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should: use strong passwords, which should be changed regularly; not write passwords down and not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or tagged on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy. School equipment for taking images is available but personal devices can be used within professional bounds and any images should be deleted from their personal devices once finished with.

Only school cameras and school iPad/tablets are to be used to capture photos/videos in the EYFS (Early Years Foundation Stage) and these are not to be removed from school; personal devices are prohibited and everyone who works in the Early Years department will keep their personal mobile phones locked away during the working day.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils are encouraged not to share, publish or distribute images of others without permission and should act responsibly if they do so.

Photographs published for school promotion purposes that include pupils will be selected

carefully, will be used according to our Terms and Conditions and will comply with good practice guidance and school policies on the use of such images. Pupils' full names should not be used anywhere on a website or blog, particularly in association with photographs that connect them directly to the school.

6. Misuse

Kent College will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Area Safeguarding Adviser, the Area Online Safety Adviser or CEOP. Any online safeguarding concerns should be reported to the Designated Safeguarding Lead.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures. The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy, or any other computer misuse where applicable.

**Complaints**

As with all issues of safety at Kent College, if a member of staff, a pupil or a parent has a complaint or concern relating to Online Safety prompt action will be taken to deal with it. Complaints should be addressed to the Online Safety Coordinator in the first instance, who will liaise with the Head and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around, Online Safety will be recorded and reported to the school's Designated Safeguarding Lead, in accordance with the school's Safeguarding Policy.