Online Safety and Mobile Devices Policy
WHOLE SCHOOL

1. INTRODUCTION

1.1 This policy applies to all pupils in the School, including those in EYFS.

1.2 Kent College recognises the Internet and other digital technologies provide a vast opportunity for children and young people to learn. They allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.3 As part of its commitment to learning and achievement, the School wants to ensure that the Internet and other digital technologies are used:

- To raise educational standards and promote pupil achievement;
- To develop the curriculum and make learning exciting and purposeful;
- To enable pupils to gain access to a wide span of knowledge and skills in a way that ensures their safety and security;
- To enhance and enrich their lives and understanding;
- To prepare pupils for a world which is increasingly dependent on digital technologies

1.4 To enable this to happen, Kent College takes a whole-school approach to online safety, which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

1.5 Kent College is committed to ensuring that all its pupils will be able to use existing, as well as up and coming technologies safely. It is also committed to ensuring that all those who work with children and young people, as well as their parents/carers, are educated as to the risks that exist so that they can take an active part in safeguarding children.

1.6 The School's Deputy Head Pastoral (also the Designated Safeguarding Lead – DSL) has overall responsibility for online safety and the wider Safeguarding Team have a key role to play in overseeing the safety of pupils online. In this, they are supported by specialist teachers and technical staff, who have an important role in maintaining a safe technical infrastructure at the School and in keeping abreast with the rapid succession of technical developments.

1.7 The ICT Strategy Committee considers online safety as part of its meetings, and discussions take place in other fora, such as SMT and HODs meetings, as appropriate.

1.8 The Network Manager is responsible for the security of the school network and for monitoring network traffic. Information system security is of paramount importance. IT system security is reviewed regularly, and virus protection will be updated regularly. The Deputy Head Pastoral (DSL) and the Network Manager jointly monitor the appropriate use of the school network by pupils, staff and visitors through both the Securus and LightSpeed systems.

1.9 The Bursar is responsible for data protection at Kent College and ensuring the School complies with legislation.

1.10 The Deputy Head Pastoral (DSL) and the Head of Prep (DDSL) are responsible for pupil behaviour, including behaviour on the school network and using digital technology. This includes responsibility for monitoring and responding to cases of cyberbullying.

1.11 All staff are ultimately responsible for monitoring pupils' use of the Internet, computers and mobile devices.

1.12 Online safety regularly forms a part of safeguarding updates and training.

1.13 This policy should be read in conjunction with the following documents:

- Child Protection including Safeguarding Policy
- Keeping Children Safe in Education 2020
- Staff Code of Conduct
- Anti-Bullying Policy
- Behaviour and Discipline Policy
- PSHE Policy
- RSE Policy
- Data Protection Policy
- Acceptable Use Policy

2. SCOPE OF POLICY

2.1 The policy applies to:

- All pupils, including those in EYFS;
- All staff, including visiting staff, Governors and volunteers;
- All aspects of the School's facilities, where they are used by voluntary, statutory or community organisations at any time.

2.2 Kent College will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- A range of policies, including acceptable use policies that are frequently reviewed and updated;
- Information to parents which highlights safe practice for children and young people when using the Internet and other digital technologies;
- Adequate training for staff;
- A culture of responsibility shared by all when using the Internet and digital technologies;
- Education aimed at ensuring safe use of Internet and digital technologies;
- Monitoring of use and reporting procedures for abuse and misuse.

3. FILTERS AND MONITORING

3.1 Kent College is dynamically filtered via the School's Internet Service Provider (ISP), an internal firewall, a managed web filter portal and an internal proxy.

3.2 In addition, the School uses Impero Education Pro. Impero makes use of keyword detection and logs any use of words or phrases which are associated with a variety of topics, such as terrorism, bullying and selfharm. These detections are logged and fed back to the DSL. Impero was developed with the assistance of numerous expert bodies, including the Internet Watch Foundation (IWF), the Anti-Bullying Alliance, Beat and the UK Council for Child Internet Safety.

4. PREVENT DUTY

4.1 All UK schools must have due regard to the need to prevent people from being radicalised or drawn into terrorism. This duty is known as the Prevent Duty. Kent College utilises Watchguard web content filtering to protect children from viewing inappropriate content on the Internet. Watchguard updates with common filtered websites from a central database updated by other Watchguard users around the globe to ensure that pupils are kept safe when browsing the Internet. Watchguard fully integrates with the Children's Internet Protection Act (CIPA) and IWF. Impero also alerts the School to the use of words and phrases on the school network associated with terrorism, extremism or radicalisation.

5. POLICIES AND PROCEDURES

5.1 The School understands that effective policies and procedures are the backbone to developing a whole school approach to online safety. The School's policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils.

5.2 The School seeks to ensure that Internet and mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

5.3 The School expects all staff and pupils to use the Internet and mobile and digital technologies responsibly and strictly according to the conditions below (for the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies, e.g. mobile phone, including Bluetooth applications, PDAs, etc.).

5.4 Users must not:

- Visit Internet sites, or make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - Indecent and/or inappropriate images;
  - Promoting discrimination of any kind;
  - Promoting racial or religious hatred;
  - Promoting illegal acts;
  - Promoting terrorism or extremist views, or designed to radicalise individuals;
  - Any other information which may be offensive to peers or colleagues, e.g. abusive images, sites which promote violence, gambling sites, etc.

5.5 The School recognises that in certain planned curricular activities, access to sites otherwise deemed inappropriate may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and senior management give permission, so that the action can be justified, if queries are raised later. Logging of such requests will be made by the Network Manager and recorded.

5.6 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative);
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist or anti-religious material;
- Material connected with violence, extremism and/or bomb making;
- Material connected with illegal taking or promotion of drugs;
- Material connected with software piracy;
- Material connected with other criminal activity.

5.7 In addition, users must not:

- Use the school network for running a private business;
- Enter into any personal transaction that involves the school network in any way;
- Visit sites that might be defamatory or incur liability on the part of the School, or adversely impact on the image of the School;
- Upload, download, or otherwise transmit (make, produce or distribute), commercial software or any copyrighted materials belonging to third parties outside of the school network, or to the school network itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - Financial information;
  - Personal information;
  - Databases and the information contained therein;
  - Computer/network access codes;
  - Business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate;
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe;
- Assist with unauthorised access to facilities or services accessible via the school network;
- Undertake activities with any of the following characteristics:
  - Wasting staff effort or networked resources, including time on end systems accessible via the school network and the effort of staff involved in support of those systems;
  - Corrupting or destroying other users' data;
  - Violating the privacy of other users;
  - Disrupting the work of other users;
  - Using the school network in a way that denies service to other users (e.g. deliberate or reckless overloading of access links or of switching equipment);
  - Continuing to use an item of networking software or hardware after the school network has requested that use cease because it is causing disruption to the correct functioning of the network;
  - Other misuse of the network, such as introduction of viruses;

- Use any mobile or digital technologies (e.g. 3G/4G) or mobile Internet services in any way to intimidate, threaten or cause harm to others;
- Use mobile or digital technologies to access inappropriate materials or encourage activities that are dangerous or illegal.

5.8 Where Securus (as provider of Internet connectivity) and/or the Kent College network become aware of an illegal act or an attempted illegal act, they will have to comply with the law as it applies and will take action directed by the Police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

5.9 Pupils who fail to adhere to the School's policies and procedures can expect to face sanctions. These may include confiscation of a mobile device for a defined period; suspension of school network privileges for a defined period; school detention; or in serious cases, temporary or permanent exclusion. See the School's Behaviour and Discipline Policy.

6. REPORTING ABUSE OR MISUSE

6.1 Every user has a duty to report abuse or misuse of the school network or of mobile devices at school by any other user. The incident should be reported to either the Deputy Head Pastoral (for the Senior School) or the Head of Prep (for the Prep School). If the abuse or misuse involves the Head of Prep or the Deputy Head Pastoral, the matter should be reported to the Headmistress. If the abuse or misuse involves the Headmistress, it should be reported directly to the Chair of Governors.

6.2 There will be occasions when a user receives abusive or inappropriate communication, or accidentally accesses a website that contains abusive or inappropriate material. When such a situation occurs, the expectation of the School is that the user will report the incident immediately to either the Head of Prep or the Deputy Head Pastoral. See Neutral Notification Policy.

6.3 The response of the School will be to take such incidents seriously and, where judged necessary, the DSL will refer details of an incident to the lead agencies involved in safeguarding children (MARU and CEOP). Pupils are taught how to report unpleasant, abusive or offensive internet content, for instance by using the CEOP Report Abuse icon or by speaking to a member of staff.

6.4 The School, as part of its safeguarding duty and responsibilities will assist and provide information and advice in support of child protection enquiries and criminal investigations.

7. SEXTING

7.1 See the School's Child Protection including Safeguarding Policy.

8. SEARCHING AN ELECTRONIC DEVICE

8.1 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 Management 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 Acceptable Use Policies and Anti-Bullying Policy.

8.2 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.

9. EDUCATION AND TRAINING

9.1 The School recognises that the Internet and other digital technologies can:

- Transform learning;
- Help to improve outcomes for children and young people;
- Promote creativity;
- Create a more exciting and challenging classroom experience;
- Be used as tool to provide continuity of education should the school be forced to close (the term close is used to refer to the closure of the site rather than an entire shut down of the school. See Appendix A for Safeguarding and Remote Learning guidance).

9.2 As part of achieving this, the School aims to provide an accessible system, with information and services online, which support personalised learning and choice. However, it realises that pupils need to be taught how to evaluate internet content and how to validate information before accepting its accuracy. They will be taught skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely and positively.

9.3 To this end, the School will:

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum;
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies when they encounter problems;
- Support parents in gaining an appreciation of Internet safety for their children and provide them with relevant information on the policies and procedures which govern the use of Internet and other digital technologies within the School.

9.4 The School's curriculum in Years 1-9 includes weekly Computing and IT lessons. The Senior School curriculum, including IT, PSHE, Form Time, assemblies and the

School's annual GRIT week, teaches pupils how to stay safe online. Particular attention is paid to helping pupils adjust their behaviours in order to reduce risks, including the safe use of electronic equipment and the Internet. The topic of online bullying is also addressed. All pupils in the Senior School read and sign the Acceptable Use Policy annually.

9.5 Teachers ensure pupils in the Prep School are aware of what is acceptable.

9.6 Staff also sign the Acceptable Use Policy as part of their induction and daily when logging in.

10. MONITORING

10.1 Monitoring the safe use of the Internet and other digital technologies goes beyond the personal use of the Internet and emails. The School recognises that in order to develop an effective whole school online safety approach there is a need to monitor patterns and trends of use inside school and outside school.

10.2 With regard to monitoring trends within the School and individual use by school staff and pupils, the School will audit the use of the Internet and email in order to ensure compliance with this policy. The monitoring practices of the School are influenced by a range of issues and guidance notes and documents produced both nationally and regionally.

10.3 Pupils are expected to connect to the school network any mobile device which they bring to school, if they intend to use the device for anything other than making phone calls. Pupils below Year 11 are not permitted to have their mobile phones on their person during the school day and are required to hand them in during morning registration.

10.4 The School is aware that pupils in Y11 to Sixth Form may choose to bypass the School's filtering systems by connecting their mobile devices to 3G and 4G. The School Rules make it clear that mobile phones should only be used in designated areas or unless a teacher has given permission for the phone to be used for a specific task. Pupils may use other mobile devices or may use phones outside of these hours. Staff understand the need to monitor pupil use of mobile devices while in school and to ensure that these are not misused. When a member of staff finds a pupil using a mobile device against school policy or the School Rules, they will confiscate the item and report the matter to a member of SMT, who will investigate and determine whether a sanction should be imposed.

10.5 Boarding staff are aware of the opportunities in the boarding houses for pupils to bypass the School's filtering systems by connecting to 3G or 4G. They monitor use closely and also run a pupil lead IT forum to enable a continual and open dialogue between staff and boarders. Younger pupils are required to hand in their mobile devices at bedtime. If boarding staff discover a pupil misusing a mobile, the item is confiscated for a period of time. Other sanctions may also be applied.

11. WORKING IN PARTNERSHIP WITH PARENTS/CARERS

11.1 The School is committed to working in partnership with parents/carers and understands the key role they play in the safety of their children online, through promoting Internet safety at home and elsewhere.

11.2 The School appreciates that there may be some parents/carers who are concerned about the use of the Internet, email and other digital technologies in the School. In such circumstances school staff will meet with parents/carers to discuss their concerns and agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe.

11.3 Where the School becomes aware of new technology or software which may pose a risk to pupils, it makes parents/carers aware of this and offers advice. This is often done via the weekly bulletin. The School also runs events for parents on online safety with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

Policy reviewed by Deputy Head Pastoral (DSL)

Governors' Committee: Education

Approved by Education Committee: March 2020

Review by Deputy Head Pastoral: September 2020

Approved by Education Committee: November 2020

Appendix A Safeguarding and Remote Learning

In the event of a school closure, this being the closure of buildings rather than complete shutdown, Kent College will continue to provide education provision to ensure continuity of learning for all pupils. This will be carried out remotely using various tools and platforms.

The following areas must be considered in order for the School to fulfil its obligation in terms of provision of education whilst also ensuring the safeguarding of staff and pupils.

i. Policy

Staff should ensure they are familiar with the following policies/documents:

- Online Safety Policy
- Child Protection Policy (including safeguarding)
- Acceptable Use Policy
- Staff Code of Conduct

Pupils must be reminded of the School's expectations for them to follow the:

- Acceptable Use Policy
- Pupil Code of Conduct
- Behaviour and Discipline Policy
- Attendance procedures

Parents should be informed of provisions for remote learning and must also ensure that they are responsible for their child/ren accessing this learning at the required times (See section iv)

ii. Resources

There are a wealth of online services and systems that enable online video and audio communication, however, where possible Kent College encourages the primary use of Firefly and ZOOM to provide remote learning to pupils. Departments may also use platforms they regularly use with classes, such as MathsWatch and Educake.

If a member of staff wishes to use an alternative platform to remotely educate their classes, they must seek prior permission from a member of the Executive Team (which comprises the Headmistress, Head of the Prep, Deputy Heads Academic and Pastoral and the Bursar) and a clear rationale and risk assessment must be completed to support their request.

Remote learning can be delivered it two ways:

- Passive or Interactive = teacher posts activities and student posts responses. e.g.: Online tutorials via Firefly, MathsWatch, Educake etc. This may also be

delivered via Podcast/voice tutorials. Staff should avoid one to one online tuition to help safeguard pupils and themselves. Staff should consider if the system they are using, includes an online chat feature, and if this can be muted.

- Active, Interactive, live or Synchronous = pupils and staff connected in the same service at the same time - i.e. live video and audio. Caution - without expertise and experience this may not be the most appropriate approach for pupils in the first instance.

Other factors for staff to consider are:

Age, Group Size and Ability: The use of remote learning platforms will also be influences by the age of the pupils, size of the group being taught and their ability. For example, larger groups of pupils may be more challenging to manage during an interactive online class and so more passive or broadcast approaches may be more suitable.

Live Video: Some staff may consider using Livestreaming services but should exercise caution here given requirements for accounts, personal data and privacy questions.

Restrictions: Staff must consider the terms of service together with privacy policies and in particular if there are any minimum age requirements of the chosen service.

Privacy Settings: Staff must consider privacy settings before posting – (e.g. YouTube has a variety of settings (Public, Unlisted, Private, Comments Allowed/Not Allowed) that will determine who can see and comment on the video).

Messaging Services: Staff must be mindful of professional standards and as such should only use the School email system or Firefly to message pupils.

iii. Technology

Although Kent College is in the fortunate position that the vast majority of their pupils will have access to the technology which will enable remote learning to take place, it is important that the School identifies any issues that both pupils and staff may have in terms of access to technology. In the event of a school closure (this being the buildings rather than complete shutdown) the Deputy Heads should ensure that any member of the community who may have difficulty with access are identified and loaned equipment. If the loaning of equipment is not possible, then a suitable alternative provision must be arranged to enable the individuals to continue being educated or to educate.

Kent College will consider activities carefully when planning for remote education as online access within school will have internet content filtering systems in place but this is unlikely to be replicated in the home environment.

Staff should be careful to check that any provision used does not incur surprising costs for both their pupils and themselves, e.g. mobile data access charges - (video utilises significant amounts of data).

The school technical teams will be remotely on hand to provide advice and answer queries. Staff should log these in the normal way, via the IT helpdesk on their remote desktop.

Staff and pupils should consider the security of devices, in particular cameras and microphones and make sure that they are only switched on for the duration of the learning session.

Staff should be vigilant when using personal laptops and computers when working remotely. They should always check to ensure that they are not sharing personal information and that they are safeguarding their pupils as well as themselves. Kent College therefore strongly recommend that staff work remotely via the school's remote desktop and approved secure platforms, such as Firefly and their school email account. In the event of a possible data breach, or any other concerns, staff are encouraged to report these to the DSL, who will make a note and advise colleagues of any remedial action required.

iv. Education

In the event of Kent College having to educate pupils remotely, the Deputy Head Academic will lead with any required staffing changes, planning, supporting and managing distance learning.

Remote learning will, wherever practicably possible continue to follow the usual school timetable, with the school day starting at 8:30am and finishing at 4:15pm. Each group within the school community will have specific roles to play and these are outlined below:

- **The Role of Staff** – Staff should ensure that they provide lesson content promptly, as would be expected during a normal school day. If a member of staff is educating passively, this should be available for the start of the lesson period. If they are educating actively, they should ensure they are logged on 5 minutes before the start of the lesson so as to begin the interaction promptly. Staff should also ensure that they have taken a register for their lesson and provided this (along with the name of the class and lesson period, e.g. L6C P1&2) to attendance at attendance@kentcollege.kent.sch.uk.
- **The Role of the Pupil –** Pupils should work to their usual school timetable, ensuring they are checking their emails regularly for communication and resources and logging into platforms when instructed to do so.
- **The Role of the Parent –** Parents responsibilities remain the same in terms of their child/ren attendance. Therefore parents must ensure that their child/ren are

up and ready for the school day and logged on ready for relevant lessons on their timetable.

Given that the reason for remote learning will likely be due to exceptional circumstances it is important that staff take into consideration any reasonable difficulties pupils may face when setting work. This may mean staff will have to either plan for a lower volume of work from students or allow for extended timescales, provide for reasonable deadlines and set marking expectations and standards, which may be different from normal. However, it is imperative that staff provide remote education which has continuity.

Kent College will work with staff and pupils to identify support and training opportunities as early as practicably possible to help everyone manage their remote teaching.

It is important for staff to plan screen-based and non-screen based activities to achieve a healthy screen time balance. It is also vital that pupils and staff are also given the opportunity for reasonable breaks, activities and relaxation. Therefore each day, the 8:30-9:00am Form/Assembly slot should have various pastoral and wellbeing activities scheduled. This, alongside the regular breaks, lunch times and Sport and Wellbeing sessions should continue to provide pupils and staff with the right balance.

v. Behaviour

Both pupils and staff are required to behave in the same manner that would be expected during a normal school day.

During scheduled lesson time, staff should maintain their classroom rules with pupils, such as arriving promptly, meeting deadlines, not interrupting, and displaying respect to others.

vi. Recording

Staff should always make a note of the conference timing and who participated, including those that arrived/departed early or late. This should be sent to attendance as stated in section iv.

Staff should be clear about whether they are comfortable for certain aspects of their remote lesson to be recorded and shared. This should be approached in the same way it is during a normal school day. It is only acceptable for students to record events and share if they have the express permission of the person being recorded.

If the service being used records the interaction/conference/tutorial, make sure that everyone is aware of this. It's important to know how long any recordings are kept for and how to access them.

vii. Personal Data

Lessons: The conference service may require the sharing of personal data, e.g. usernames to invite in. It is always best practice to use school-provided email addresses as Data protection laws still apply.

Parental communication: Unless a member of staff has a school device for making telephone calls, they should only communicate with parents via email during remote education periods.

viii. Safeguarding

If live video and audio is being used, there should be careful consideration of the location that everyone uses. It is possible that pupils may be in their bedrooms and this may not be appropriate. You may choose to use a conferencing service that the teacher can disable users' microphone and video cameras.

During live video sessions with classes, both staff and pupils are expected to dress appropriately. They do not have to wear uniform or business attire but should be dressed respectfully. As would be the case during a normal school day, staff have the right to ask a pupil to adjust their attire if they deem it unacceptable. As a rule of thumb, staff and pupils should consider what would be acceptable attire for a home clothes day.

Online or offline, effective Safeguarding requires a whole-school approach. The planning for online or distance learning activities should include the school's safeguarding team as part of the planning process.

Ensure online tuition follows best practice (e.g. 2 members of staff involved) and is in-line with the School's Child Protection including Safeguarding Policy, Online Safety Policy, Staff Code of Conduct

Staff must maintain their safeguarding obligations. Record any safeguarding incidents or potential concerns on CPOMs. In the event of a Child Protection issue, staff should call the Deputy Head (DSL) directly on 07984 322122.

During periods of remote education, pupils should be reminded of who they can contact within the school for help or support. These key members of staff should email pupils with this message reminding them that they are available via email.