Dream, Believe, Persevere, Achieve

Cape Cornwall School

E-Safety Policy

School Name: Cape Cornwall School

Dissemination: Website and O: Drive

Date policy approved by Governors: November 2018

Date policy becomes effective: Immediately

Review date: November 2020

Person responsible for Implementation and Monitoring: Designated Safeguarding Lead (DSL)

Links to other relevant policies: Behaviour, Safeguarding, Anti-Bullying, Data Protection, Acceptable Use (ICT).

1. Aims

Cape Cornwall School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Governors.
- Have an effective approach to online safety which protects and educates the whole school community in the safe use of technology.
- Establish clear mechanisms to identify, intervene in and escalate an incident of inappropriate use of technology, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, *'Keeping Children Safe in Education'*, and advice for schools on preventing and tackling bullying including; searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which gives teachers stronger powers to tackle cyber bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a good reason to do so.

3. Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed by Cape Cornwall

School as part of our wider duty of care to which all who work in our school are bound. Our E-safety policy helps to ensure safe and appropriate use. The successful implementation of this policy will involve all the stakeholders in our school including the Head of School and Governors, senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

The use of technologies in our school and at home has been shown to raise educational standards and promote student achievement. However, the use of technologies can put young people at risk within and outside of school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content,
- Unauthorised access to/loss of/sharing of personal information,
- The risk of being subject to grooming by those with whom they make contact on the internet,
- The sharing/distribution of personal images without consent or knowledge,
- Inappropriate communication/contact with others, including strangers,
- Cyber-bullying,
- Access to unsuitable video/internet games/images,
- An inability to evaluate the quality, accuracy and relevance of information on the internet,
- Plagiarism and copyright infringement,
- Illegal downloading of music or video files,
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this E-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' awareness to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. This E-safety policy explains how we intend to do this, while also addressing wider educational issues in order to help our young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

4. Scope of the Policy

This policy applies to all members of Cape Cornwall School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of our school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary sanctions for inappropriate behaviour. This is relevant to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

Cape Cornwall School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviours that take place in and out of school.

5. Roles and Responsibilities

The following section outlines the roles and responsibilities for E-safety of individuals and groups within the school:

Governors

Governors are responsible for the review and approval of the E-Safety Policy and ensure its effective application. This will be carried out by the Governors Committee. The Safeguarding Governor has responsibility for meeting with the Designated Safeguarding Lead (DSL)to review the implementation of this policy.

Head of School and Senior Leaders

- The Head od School is responsible for ensuring the safety (including E-safety) of members of the school community. The day to day responsibility for E-safety is delegated to the DSL and DDSL (Deputy Designated Safeguarding Lead).
- The Head of School is responsible for ensuring that the DSL/DDSL and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
- The Head of School/Senior Leaders ensure that there is a system in place to allow for monitoring and support of those in school who carry hold responsibility for E-safety. This is to provide a safety net and also support to those colleagues who take on important roles.
- The Senior Leadership Team will receive reports from the DSL/DDSL.
- The Head of School and other members of the Senior Leadership team will carry out the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff. (see flowchart on dealing with E-safety incidents – "Responding to incidents of misuse").

Designated Safeguarding Lead (DSL)

- Has day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies/documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place;
- provides training and advice for staff;
- liaises with school ICT technical staff;
- receives reports of E-safety incidents (logged in SIMs) to inform future E-safety developments;
- reports regularly to Senior Leadership Team.

Network Manager/Technical staff

The Network Manager is responsible for ensuring:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Trust or Local Authority E-Safety Policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- SWGfL is informed of issues relating to the filtering applied by the Grid.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

- He/she keeps up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant.
- The use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the DSL/Head of School for investigation/action/sanction.
- Monitoring software/systems are implemented and updated.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of E-safety matters and of the current school E-safety policy and practices.
- They have read, understood and signed the school Staff Acceptable Use Policy/Agreement.
- They report any suspected misuse or problem to the ICT Network Manager/DSL /Head of School/Senior Leader/Head of Year for investigation/action/sanction.
- Digital communications with students/parents (email/Virtual Learning Environment (VLE)) must be on a professional level using school email systems/ICT systems.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Students understand and follow the school E-safety and Acceptable Use Policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned, students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguard Lead (DSL) and Safeguarding Team

The safeguarding team are trained in E-safety issues and aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Cyberbullying.
- Radicalisation.

Students

Students at the school should:

- Use the school ICT systems in accordance with the Student Acceptable Use Policy.
- Avoid plagiarism and uphold copyright regulations.
- Report abuse, misuse or access to inappropriate materials.
- Comply with Cape Cornwall School policies on the use of mobile phones, digital cameras and handheld devices and understand the school policies on the taking/use of images and on cyberbullying.

- Adopt good E-safety practice when using digital technologies out of school and comply with the school's E-Safety Policy in their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Cape Cornwall School will help parents understand these issues through parents' evenings, newsletters, and website. Parents and carers will be responsible for:

- Upholding the Student Acceptable Use Policy.
- Accessing the school website in accordance with the relevant school Acceptable Use Policy.
- Supporting the school in resolving any E-safety incidents.

Policy Statements

6a. Education – students

The education of students in E-safety is an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned E-safety programme will be provided and will be regularly reviewed – this will cover both the use of ICT and new technologies in school and outside school.
- Students will be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

6b. Education and Training – Staff

All staff will receive appropriate E-safety training and understand their responsibilities. Training will be offered as follows:

- All new staff will receive E-safety training information as part of their induction programme, this should ensure that they fully understand the school E-safety policy and Acceptable Use Policies.
- The DSL (or other nominated person) will receive regular updates through attendance at SWGfL/LA/Trust information/training sessions.
- The DSL (or other nominated person) will provide regular updates for staff and will provide advice/guidance/training as required to individuals.

6c. Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections are effective in carrying out their E-safety responsibilities.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Trust or Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems by the Network Manager.
- Servers, wireless systems and cabling will be securely located and physical access to them restricted.
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password. The user is responsible for the security of their username and password and must not allow other users to access the systems using their log on details. Staff must immediately report any suspicion or evidence that there has been a breach of security to the Network Manager.
- The "administrator" account for the school ICT system, used by the ICT Network Manager (or other person) will also be available to the Head of School or other nominated senior leader.
- The school maintains and supports the managed filtering service provided by SWGfL.
- The school provides enhanced user-level filtering through the use of a filtering programme.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out the agreed process.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed annually by the DSL.
- School ICT technical staff monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users' activity.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, handheld devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (See Acceptable User Policies).

6d. Curriculum

E-safety is a focus in all areas of the curriculum and teachers and support staff will reinforce E-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be logged, with clear reasons for the need.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

6. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement strategies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate students about the risks associated with the taking, using, 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.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images may only be taken on school equipment and the personal equipment of staff must not be used for such purposes (see Staff Acceptable Use Policy).
- Care must be taken when taking/using digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their consent.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used on the website, school's social media or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media.
- Students' work can only be published with the permission of the student and parents or carers.

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the GDPR regulations and Data Protection Act 1998, which states that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media, the data must be encrypted and password protected. See Data policies for more detail.

8. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Appendix 1 shows how the school currently considers the benefit of using these technologies for education outweighing their risks/disadvantages. When using communication technologies, the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Staff and students must therefore use **only** the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Email communications are monitored.
- Users must immediately report to the DSL or ICT Network Manager, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (via school email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications (See Acceptable Use Policy).
- Students are taught about email safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information must not be posted on the school website and only official email addresses should be used to identify members of staff.

9. Unsuitable/Inappropriate activities

Cape Cornwall School believes that there are activities (referred to in Appendix 2) that would be inappropriate in a school context and that users must not engage in identified activities in school or outside school when using school equipment or systems.

10. Responding to incidents of misuse

All members of the school community are expected to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy may take place, through careless, irresponsible or, through deliberate misuse. Listed below are the responses that will be made to any incident of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e:

- Child sexual abuse images.
- Adult material, which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

The SWGfL flow chart (Appendix 3) and http://www.swgfl.org.uk/safety/default.asp will be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.
If members of staff suspect that misuse might have taken place, in or out of school, it impacts school life and/or its community including bringing the school into disrepute but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one member of staff will be involved in the investigation which will be carried out on a "clean" designated computer. It is important that any incidents are dealt with as soon as possible, in a proportionate manner and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. The ICT Network Manager and Senior Leaders will be involved in the investigation as appropriate and in accordance with the decisions of the Head of School.

Appendix 1: Communications

The table below shows how the school currently considers the benefit of using these technologies for education outweighing their risks/disadvantages:

	Staff, Visitors/Volunteers				Students			
Guidance for use of personal communication devices (e.g. smartphones and watches)	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons				✓			✓	
Use of mobile phones in social time				✓				✓
Taking photos on mobile phones				✓			✓	
Taking photos on other camera devices			✓				✓	
Use of handheld devices eg PDAs, PSPs				✓				✓
Use of e-readers				✓			✓	
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities				✓				✓
Use of instant messaging				✓				✓
Use of school social networking sites (not personal sites)	✓						✓	
Use of school blog	✓						✓	
Use of personal social networking sites				✓				✓
Use of personal blogs				✓				✓

Please note mobile/smart phones are only to be used in lessons by students when no alternative technology is available and only with the permission of the teacher. As a general rule, use of personal mobile phones in school is not allowed. See Mobile Phone Policy for more details.

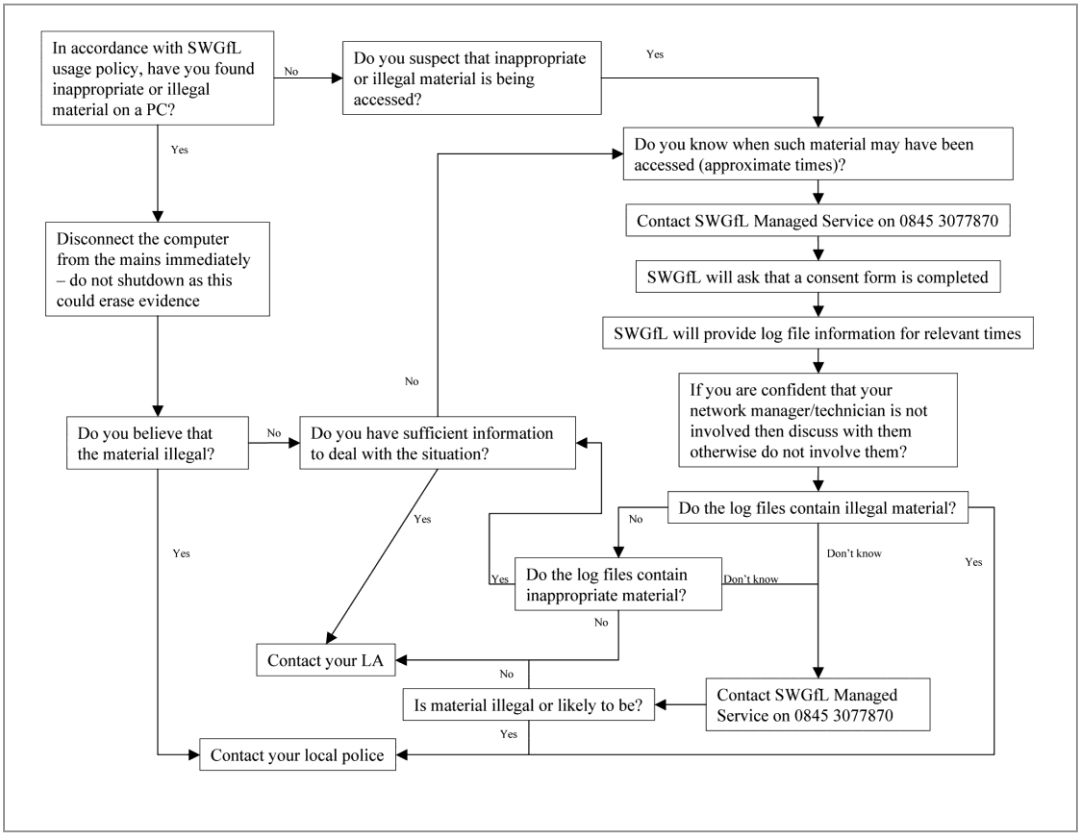
Appendix 2: Unsuitable/inappropriate activities

The school believes that the activities referred to in Appendix 2 would be inappropriate in a school context and that users should not engage in identified activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)			✓			
On-line gaming (non educational)					✓	
On-line gambling					✓	
On-line shopping / commerce, other than for school purposes					✓	
File sharing, other than for school purposes					✓	
Use of social networking sites, other than for school purposes					✓	
Use of video broadcasting e.g. YouTube, other than for school purposes					✓	

Appendix 3: Unsuitable/inappropriate activities

The SWGfL flow chart (Appendix 3) and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



Acknowledgement

This School E-Safety Policy is based on the guidance provided by SWGfL School E-Safety Policy Template.

Appendix 4: Mobile Phone Policy

Aims:

- **To provide a safe learning environment for students;**
- **To protect the dignity and professional standards of our shared workplace for staff and students;**
- **To educate young people about appropriate use of mobile phones (and similar technology) in a work environment.**

Section 1: Introduction

The school understands and accepts that the use of mobile phones (and similar technology e.g. i watches) is an integral part of the modern, digital world. Mobile phone technology can be a valuable tool for communication, time management and access to information. Mobile phone use in school is managed to ensure an orderly, safe learning environment for all students. We take our commitment to safeguarding students and to educating students about appropriate use of mobile phones in a work environment very seriously.

The inappropriate use of mobile phones is rare in our school community. Where we have dealt with inappropriate use, we know that the resulting negative impact on students can be significant and long lasting. The support of parents, staff and students regarding appropriate use is very much appreciated.

Parents and Carers are reminded that there is no evidence that carrying a mobile phone offers any level of protection to students on the way to, or from, school.

Section 2: Management of Mobile Phones in School (Students)

Students who bring phones to school do so at their own risk. The school does not accept responsibility for loss or damage to phones brought to school. Lockers are available to provide a safe place for students to store their belongings. Where phones are brought into school, they must be switched off and kept in student bags (specifically not in pockets).

Students should not wear headphones during the school day, during lessons or social times unless specifically told to do so by a member of staff as an integral part of the lesson.

The school network and internet connection are not available to students' personal devices including mobile phones.

Mobile phones should not be used during the school day. This applies to students on site before the official start to the school day, registration, lesson time, break, lunchtime and after school provision (e.g. clubs, revision classes). This applies to all areas of the school site: classrooms, social spaces, corridors and the grounds.

With specific permission from the teacher, phones may be used in lessons to support lesson activities where this is an essential and integral part of the lesson. Mobile phones should only be used where there is no better alternative available and where the technology is an invaluable part of learning. The student must ask the teacher for permission to use their phone for this activity which must be directly related to the purpose of the lesson. Only with permission may students use their phones during lesson time. Mobile phones should not be used as timers or calculators as these functions are much better resourced by specialist equipment (scientific calculators and stop clocks).

Mobile phone or smartwatch use which interrupts school activities e.g. phones ringing during lesson time, or use during break time, will be sanctioned using the Behaviour Policy. Phones used inappropriately will be confiscated and held securely in the Main Office for collection on the first occasion by the students from 3.00pm onwards and, if there is a repeat confiscation, by a parent/carer from 3.00pm onwards. Confrontational behaviour as a result of mobile phone confiscation will receive further sanctions.

In particular, students are not allowed to take images (photo or video) of other students at any time during the school day. Photos of students in uniform and/or linked to Cape Cornwall School activities, must not be posted onto social media sites. Damage to the school's reputation as a result of breaches to this policy will be taken very seriously by staff and Governors and may result in significant sanctions including exclusion from school.

Where the school is aware that a students' phone has been used inappropriately, students may be required to delete inappropriate images and content from their phones including images on social media sites. Where appropriate, phones may be given to the police for further investigation. This applies to phone use that has taken place in school during the school day and, where appropriate, to phone use that has taken place outside school which has involved members of the school community.

Where phone use may be illegal e.g. cyberbullying, threats of physical aggression or inappropriate images, the school has a duty to refer the incident to the police and the student's phone may need to be given to the police for further investigation. Please contact a member of our safeguarding team if you have any concerns. Details are on our website or available through Reception.

Where a student repeatedly fails to follow the school policy regarding use of mobile phones, the school may remove the student's privilege to bring a phone to school.

Students are reminded that if an incident occurs in school, a member of school staff will contact parents.

Where students need to contact home (e.g. to check transport arrangements or to ask parents to bring equipment or lunch money to school) students should ask at Reception to use the school phone to contact home. The school does not charge students for phone calls to parents/carers.

Parents/carers needing to contact students during the school day should phone Reception and a member of school staff will ensure that students are informed as soon as possible. Parents are asked not to phone or text students directly during the school day to ensure that students do not receive sanctions for use of their phone. In addition, we would like to remind parents that in a family emergency or crisis, students may need staff support and that contacting students through Reception ensures that staff are in a position to support students as needed.

Students will be given clear information about the use of their phone whilst on a school trip or participating in a school event by the school leader. Phones should only be used on a school trip with explicit permission from the trip leader and for a purpose directly linked to the educational aim of the trip. The school appreciates that students' mobile phones can be a useful and valuable means of communication with parents during a school trip.

Section 3: Management of Mobile Phones in School (Staff)

Staff use of mobile phones must be discreet and should take place in a private area unseen (and unheard) by students e.g. staff room or office. Staff mobile phones must not be used in classrooms at any time when students are present. Staff mobile phones must be kept securely e.g. in a locked cupboard and must be protected by an appropriate pin-code (or similar). Official school mobile

phones are available for trips and visits. Staff must not give their personal telephone number to students or parents and all communication must take place through official school email, or telephone contacts. Staff must not lend their mobile phones to students. For more details on staff use of phones, please see Professional Codes of Conduct. These rules apply to all staff (paid and voluntary) and to Governors.

The school does not accept responsibility for loss or damage to staff phones.

Section 4: Management of Mobile Phones (Visitors)

Visitors to the school are not permitted to use their mobile phones on the school site for any reason during the school day. Visitors should ask a member of staff for assistance if they need to use a phone. All staff are expected to be vigilant about the use of mobile phones by visitors and to challenge use of phones by visitors to the school. This includes the use of mobile phones by parents during the school day whilst on school site.

Parents must not take images (photos or video) of students participating in school events e.g. sports fixtures, concerts, other performances. Parents will be reminded of this rule at the event by a member of school staff.

During school holidays, when students are not in school, visitors (e.g. contractors) are allowed to use mobile phones.

The school does not accept responsibility for loss or damage to visitor phones.

Please contact a member of our safeguarding team if there any concerns. Details are on our website or available through Reception.

Examples of situations that will lead to confiscation of a phone:

- A phone disrupts a school activity e.g. rings during assembly, used in a lesson without permission. This also applies to similar technology e.g. i watches;
- a student is using a phone without permission during the school day e.g. in a corridor, classroom or in the school grounds;
- a student takes a photo or video of another student;
- there are inappropriate photos on the phone or the phone has been used inappropriately e.g. cyber bullying;
- phone is used without permission in lessons.