RIPPLEVALE
SCHOOL

Online Safety Policy

Date of issue: 13.02.2023

Review Cycle: Annual

Next Review Date: February 2024

Ripplevale School is owned and operated by Cavendish Education.

This policy is one of a series of school policies that, taken together, are designed to form a comprehensive statement of the school's aspiration to provide an outstanding education for each of its students and of the mechanisms and procedures in place to achieve this. Accordingly, this policy should be read alongside these policies. In particular it should be read in conjunction with the policies covering equality and diversity, Health and Safety, safeguarding and child protection.

All of these policies have been written, not simply to meet statutory and other requirements, but to enable and evidence the work that the whole school is undertaking to ensure the implementation of its core values:

Ripplevale School provides a caring learning environment where our students make meaningful progress, relative to their individual starting points. Our aim is to encourage them to develop appropriate personal, social and employable skills enabling them to become confident, independent and aspiring young people

While this current policy document may be referred to elsewhere in Ripplevale School documentation, including particulars of employment, it is non-contractual.

In the school's policies, unless the specific context requires otherwise, the word "parent" is used in terms of Section 576 of the Education Act 1996, which states that a 'parent', in relation to a child or young person, includes any person who is not a biological parent but who has parental responsibility, or who has care of the child. Department for Education guidance Understanding and dealing with issues relating to parental responsibility considers a 'parent' to include:

- all biological parents, whether they are married or not
- any person who, although not a biological parent, has parental responsibility for a child or young person - this could be an adoptive parent, a step-parent, guardian or other relative
- any person who, although not a biological parent and does not have parental responsibility, has care of a child or young person.

A person typically has care of a child or young person if they are the person with whom the child lives, either full or part time and who looks after the child, irrespective of what their biological or legal relationship is with the child.

The school employs the services of the following consulting companies to ensure regulatory compliance and the implementation of best practice:

- Peninsula BrightHR
- Peninsula BusinessSafe (Health and Safety)
- Atlantic Data (DBS)
- Educare (online CPD)
- SchoolPro (GDPR)

Ripplevale School is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, pupils and visitors to share this commitment.

All outcomes generated by this document must take account of and seek to contribute to safeguarding and promoting the welfare of children and young people at Ripplevale School.

The policy documents of Ripplevale School are revised and published periodically in good faith. They are inevitably subject to revision. On occasions a significant revision, although promulgated in school separately, may have to take effect between the re-publication of a set of policy documents. Care should therefore be taken to ensure, by consultation with the Senior Leadership Team, that the details of any policy document are still effectively current at a particular moment.

1 Purpose and policy scope

Ripplevale School [the School] believes that:

1. Online safety (e-Safety) is an essential element of safeguarding children and young people and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
2. The internet and information communication technologies are an important part of everyday life, so children and young people must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
3. The School has a duty to provide the community with quality internet access to raise education standards, promote achievement, support the professional work of staff and enhance leadership functions.

4. There is a clear duty to ensure that all children and young people and staff are protected from potential harm online.

1.1 The purpose of the School's *Online Safety Policy*

1. To clearly identify the key behaviours expected of all members of the community with regards to the safe and responsible use of technology to ensure that the School is a safe and secure environment.
2. To safeguard and protect all members of the School community online.
3. To raise awareness with all members of the community regarding the potential risks as well as benefits of technology.
4. To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
5. To identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

1.2 Scope

This Policy applies to all staff, including the senior leadership team (SLT), 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'), as well as children and young people and parents/carers.

This Policy applies to all access to the internet and use of information communication devices, including personal devices (see below for information regarding the use of personal devices), or where children and young people, staff or other individuals have been provided with school-issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This Policy must be read in conjunction with other relevant school policies including (but not limited to) the School *Safeguarding Policy* and *Child Protection Policy*, *Anti-Bullying Policy*, *Behaviour Policy*, *Data Protection Policy*, image use policies for staff, visitors and for students, confidentiality and privacy notices for staff and students, and relevant curriculum policies including computing, Personal Social Health and Economic Education (PSHE), Relationships Education (RE) and Relationships and Sex Education (RSE).

2 Responsibilities

The Designated Safeguarding Lead (DSL) is Jane Norris.

The School Online Safety Policy has been written by the School, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.

The School has appointed the DSL as an appropriate member of SLT alongside the online safety lead (IT Manager).

The *Online Safety Policy* and its implementation will be reviewed by the School at least annually or sooner if required.

2.1 Key responsibilities - people

2.1.1 SLT

1. Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
2. Ensuring that online safety is viewed by the whole School community as an integral component of safeguarding and proactively developing a robust online safety culture.
3. Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
4. Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including acceptable use of ICT policies which cover appropriate professional conduct and use of technology.
5. Ensuring that suitable and appropriate filtering and monitoring systems are in place to protect children and young people from inappropriate content which meet the needs of the School community whilst ensuring children and young people have access to required educational material.
6. Working with and supporting staff in monitoring the safety and security of School systems and networks and to ensure that the School network system is actively monitored.
7. Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications – in line with the School's National Online Safety Accreditation.
8. Ensuring that online safety is embedded within a progressive whole-school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
9. Being aware of any online safety incidents and ensuring that external agencies and support are liaised with as appropriate.
10. Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
11. Ensuring there are robust reporting channels for the School community to access regarding online safety concerns, including internal, local and national support.
12. Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
13. Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

2.1.2 DSL

1. Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
2. Keeping up-to-date with current research, legislation and trends regarding online safety.
3. Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
4. Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches. This includes the school website which has regular updates of newsletters.
5. Working with the School lead for data protection and data security (**IT Manager**) to ensure that practice is in line with current legislation.

6. Maintaining a record of online safety concerns/incidents and actions taken as part of the School's safeguarding recording structures and mechanisms.
7. Monitoring the School's online safety incidents to identify gaps/trends and use this data to update the School's education response to reflect need.
8. Reporting to SLT and other agencies as appropriate, on online safety concerns and local data/figures.
9. Liaising with the local authority and other local and national bodies, as appropriate.
10. Working with SLT to review and update the *Online Safety Policy* and procedures, and other related policies on a regular basis (at least annually), with stakeholder input.
11. Ensuring that online safety is integrated with other appropriate School policies and procedures.

2.1.3 Staff

1. Contributing to the development of online safety policies.
2. Reading the school's IT policies and adhering to them.
3. Taking responsibility for the security of School systems and data.
4. Having an awareness of a range of different online safety issues and how they may relate to the children and young people in their care.
5. Modelling good practice when using new and emerging technologies.
6. Embedding online safety education in curriculum delivery wherever possible.
7. Identifying individuals of concern and taking appropriate action by following the *School Safeguarding Policy* and procedures.
8. Knowing when and how to escalate online safety issues, internally and externally.
9. Being able to signpost appropriate support available for online safety issues, internally and externally.
10. Maintaining a professional level of conduct in their personal use of technology, both on and off site.
11. Demonstrating an emphasis on positive learning opportunities.
12. Taking personal responsibility for professional development in this area.

2.1.4 IT Consultants (SDS Ltd.)

1. Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
2. Taking responsibility for the implementation of safe security of systems and data in partnership with SLT.
3. Ensuring that suitable access controls and encryption are implemented to protect personal and sensitive information held on school-owned devices.
4. Ensuring that the School's filtering system is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
5. Ensuring that the use of the School's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
6. Reporting any breaches or concerns to the DSL and SLT and together ensuring that they are recorded and appropriate action is taken as advised.
7. Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
8. Providing technical support and perspective to the DSL and SLT, especially in the development and implementation of appropriate online safety policies and procedures.

9. Ensuring that the School's ICT infrastructure/system is secure and not open to misuse or malicious attack.
10. Ensuring that appropriate anti-virus software and system updates are installed and maintained on all School machines and portable devices.

2.1.5 Students

1. Taking responsibility for keeping themselves and others safe online.
2. Contributing to the development of online safety policies.
3. Respecting the feelings and rights of others both on and offline.
4. Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
5. Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2.1.6 Parents and carers

1. Reading the School's Acceptable Use of IT Policy - Student, encouraging their children and young people to adhere to them, and adhering to them themselves where appropriate.
2. Discussing online safety issues with their children and young people, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
3. When/if students are involved in remote learning: Teachers should communicate clearly to parents/carers what they are asking their students to do online. Parents/carers should be informed of what searches etc. are expected and should be available to give advice to parents/carers about ensuring on-line safety whilst carrying out remote learning. Teachers must ensure that they use appropriate forms of communication with parents/carers and that they can confirm that parents/carers have received this information.
4. Role modelling safe and appropriate uses of technology and social media.
5. Identifying changes in behaviour that could indicate that their child is at risk of harm online.
6. Seeking help and support from the School, or other appropriate agencies, if they or their child encounters online problems or concerns.
7. Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

2.2 Key responsibilities - systems

2.2.1 Managing the school website

1. The School will ensure that information posted on the School website meets the requirements as identified by the Department for Education (DfE).
2. The contact details on the website will be the School address, email and telephone number. Staff or students' personal information will not be published.
3. The Head of School will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
4. The website will comply with the School's guidelines for publications including accessibility, respect for intellectual property rights, privacy policies and copyright.
5. Email addresses will be published carefully online, to avoid being harvested for spam.
6. Students' work will only be published with their permission or that of their parents/carers.
7. The administrator account for the school website will be safeguarded with an appropriately strong password.

8. The School will post information about safeguarding, including online safety, on the School website for members of the community.

2.2.2 Publishing images and videos online

1. The School will ensure that all images and videos shared online are used in accordance with the School's use of photographic images policy.
2. The School will ensure that all use of images and videos takes place in accordance with other policies and procedures including: *Data Protection Policy*; *Acceptable Use of IT Policies* and *Staff Codes of Conduct*. In line with our use of photographic images policy, written permission from parents or carers will always be obtained before images/videos of students are published electronically.

2.2.3 Managing email

1. Students may only use School-provided email accounts for educational purposes.
2. All members of staff are provided with a specific School email address to use for any official communication.
3. The use of personal email addresses by staff for any official School business is not permitted.
4. The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
5. Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will be sent only to recipients who are authorised to receive it (under GDPR rules) - if necessary, with password protection.
6. Access to School email systems will always take place in accordance with data protection legislation and in line with other appropriate School policies and procedures, e.g. GDPR rules.
7. Members of the community must immediately tell SLT or the IT Manager if they receive offensive communication and this will be recorded in the School safeguarding files/records.
8. Excessive social email use can interfere with teaching and learning and will be restricted. Access in School to external personal email accounts may be blocked.
9. School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.2.4 Appropriate and safe classroom use of the internet and any associated devices

1. Internet use is a key feature of educational access and all children and young people will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
2. The School's internet access is designed to enhance and extend education.
3. Access levels to the internet are reviewed to reflect the curriculum requirements and the age and ability of students.
4. All members of staff are aware that they cannot rely on filtering alone to safeguard children and young people and supervision, classroom leadership and education about safe and responsible use are essential.
5. Supervision of students will be appropriate to their age and ability.
6. All students are appropriately supervised when using technology, according to their ability, age and understanding.

7. All school-owned devices will be used in accordance with the School's *Acceptable Use of IT Policies* and with appropriate safety and security measures in place.
8. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending them for use at home.
9. Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
10. The School will use age-appropriate search tools.
11. The School will ensure that the use of internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
12. Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
13. The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-School requirement across the curriculum.
14. The School will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

2.2.5 Use of social media

2.2.5.1 Use of social media - general

1. Expectations regarding safe and responsible use of social media will apply to all members of the School community and exist in order to safeguard both the School and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multi-player online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
2. All members of the School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
3. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the School community through regular staff meetings and emails.
4. All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
5. The School will control student and staff access to social media and social networking sites whilst on site and when using School-provided devices and systems.
6. The use of social networking applications during School hours for personal use is not permitted. Inappropriate or excessive use of social media during School/work hours or whilst using School devices may result in disciplinary or legal action and/or removal of internet facilities.
7. Any concerns regarding the online conduct of any member of the School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as the *Anti-Bullying Policy*, *Managing Allegations against Staff Policy*, *Behaviour Policy*, *Safeguarding Policy* and *Child Protection Policy*.
8. Any breaches of School policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the breaches committed. Action taken will be in accordance with relevant policies, such as the *Anti-Bullying Policy*, *Managing Allegations against Staff Policy*, *Behaviour Policy*, *Safeguarding Policy* and *Child Protection Policy*.

2.2.5.2 Use of social media – staff

1. The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
2. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the School's *Acceptable Use of IT Policies*.
3. All members of staff are advised not to communicate with or add as 'friends' any current or past children and young people/students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this must be discussed with the DSL.
4. If on-going contact with students is required once they have left the school roll, members of staff will be expected to use official school provided communication tools.
5. All communication between staff and members of the School community on School business will take place via official approved communication channels.
6. Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted.
7. Any communication from students/parents received on personal social media accounts will be reported to the School's DSL.
8. Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will **not** be shared or discussed on personal social media sites.
9. All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
10. All members of staff are encouraged to consider carefully the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with School policies and the wider professional and legal framework.
11. Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
12. Members of staff will notify SLT immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School.
13. Members of staff are encouraged not to identify themselves as employees of the School on their personal social networking accounts. This is to prevent information on these sites from being linked with the School and also to safeguard the privacy of staff members and the wider community.
14. Members of staff will ensure that they do not represent their personal views as that of the School on social media.
15. School email addresses will not be used for setting up personal social media accounts.

2.2.5.3 Use of social media – students

1. Safe and responsible use of social media sites will be outlined for children and young people and their parents as part of the *Acceptable Use of IT Policies*.

2. Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age-appropriate sites which have been risk assessed and approved as suitable for educational purposes.
3. Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
4. Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
5. Students will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
6. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
7. Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.
8. Any official social media activity involving students will be moderated by the School where possible.
9. The School is aware that many popular social media sites state that they are not for children and young people under the age of 13, therefore the School will not create accounts within School specifically for children and young people under this age.
10. Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at School, will be dealt with in accordance with existing School policies including the *Anti-Bullying Policy* and *Behaviour Policy*.
11. Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at School, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

2.2.6 Use of personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among students and staff will require all members of the School community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the School and is covered in this document and the Staff Code of Conduct.

The School recognises that personal communication through mobile technologies is an accepted part of everyday life for children and young people, staff and parents/carers but requires that such technologies need to be used safely and appropriately within the School.

2.2.6.1 Expectations

1. All use of personal devices and mobile phones will take place in accordance with the law and other appropriate School policies.
2. Electronic devices of all kinds that are brought on site are the responsibility of the user at all times. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.

3. Mobile phones and personal devices are not permitted to be used by students during the school day. Post-16 students are permitted to use mobile phones and personal devices during their break times (within the designated Post-16 area).
4. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the relevant discipline/behaviour policies.
5. Members of staff will be issued with a work phone number and email address where contact with students or parents/carers is required. If it is not possible to use a School device, members of staff will withhold their personal numbers when making phone calls on behalf of the School.
6. All members of the School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
7. All members of the School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
8. All members of the School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the School's policies.

2.2.6.2 Use of personal devices and mobile phones – staff

1. Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the School in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
2. Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and young people and will only use work-provided equipment for this purpose.
3. Staff will not use any personal devices directly with children and young people and will only use work-provided equipment during lessons/educational activities. Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SLT in emergency circumstances Staff are permitted to use mobile phones and personal devices during their break times (within the designated staff-only areas).
4. Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law, e.g. data protection, as well as relevant School policies and procedures, e.g. the *Data Protection Policy*, *Acceptable Use of IT Policies*, etc.
5. Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
6. Staff will ensure that any content bought on site via mobile phones and personal devices is compatible with their professional role and expectations.
7. If a member of staff breaches the School policy, disciplinary action will be taken.
8. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the Police will be contacted.
9. Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the School *Managing Allegations against Staff Policy*.

2.2.6.3 Use of personal devices and mobile phones – students

1. Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
2. All use of mobile phones and personal devices by children and young people will take place in accordance with the *Acceptable Use of IT Policy - Students*.
3. Students' personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons. Mobile phones or personal devices will not be used by students during lessons or formal school time. Post-16 students may use their devices in timetabled break times within the designated Post-16 areas. Post-16 students must not use their devices in the company of students in the primary or secondary areas.
4. If a student needs to contact his parents/carers, they will be allowed to use a School phone.
5. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the School office. Exceptions may be permitted by SLT on a case-by-case basis.
6. Students should protect their phone numbers by only giving them to trusted friends and family members.
7. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
8. Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
9. If a student breaches the School policy, the phone or device will be confiscated and will be held in a secure place in the School office. Mobile phones and devices will be released to parents/carers in accordance with the School policy.
10. School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the School's *Behaviour Policy* or *Anti-Bullying Policy* or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of SLT with the consent of the student or parent/carer and content may be deleted or requested to be deleted, if appropriate. In the case of sexting, the device must be handed to the DSL and no one should view the (alleged) image(s) or delete them. In this case, the DSL will contact the Police and they will take the necessary steps to determine whether the image(s) falls into the sexting category. Searches of mobile phones or personal devices will only be carried out in accordance with School policy.
11. If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the Police for further investigation (see sexting above, for example).

2.2.6.4 Use of personal devices and mobile phones – visitors

1. Parents/carers and visitors must use mobile phones and personal devices in accordance with the School's *Acceptable Use of IT Policy - Staff*.
2. Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the School use of photographic images policy.
3. The School will inform visitors of expectations of use.
4. Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

2.2.7 Reducing online risks

1. The School is aware that the internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
2. Emerging technologies will be examined for educational benefit and SLT will ensure that appropriate risk assessments are carried out before use in School is allowed.
3. The School will ensure that appropriate filtering and monitoring systems are in place to prevent staff and students from accessing unsuitable or illegal content.
4. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a School computer or device.
5. The School will audit technology use to establish if the *Online Safety Policy* is adequate and that the implementation of the policy is appropriate.
6. Methods to identify, assess and minimise online risks will be reviewed regularly by SLT and the IT Manager.
7. The School will provide an *Acceptable Use of IT Policy - Staff* for any guest/visitor who needs to access the School computer system or internet on site.
8. The school will maintain a current record of all staff and students who are granted access to the school's devices and systems. All staff and students will read and sign the relevant *Acceptable Use of IT Policy* before using any School resources.
9. Parents will be informed that students will be provided with supervised internet access which is appropriate to their age and ability.
10. Parents will be asked to read the *Acceptable Use of IT Policy - Student* for student access and discuss it with their child, where appropriate. This is sent to parents with the School's new student information pack.
11. The School will make decisions on internet use based on the specific needs and understanding of the student(s).
12. An online safety (e-Safety) curriculum will be established and embedded throughout the whole School, to raise awareness regarding the importance of safe and responsible internet use amongst students.
13. Education about safe and responsible use will precede internet access.
14. Students' input will be sought when writing and developing School online safety policies, including curriculum development and implementation, as part of our on-line safety committee.
15. Parents are asked to support their children and young people in reading and understanding the *Acceptable Use of IT Policy - Student* in a way which suits their age and ability.
16. All users will be informed that network and internet use will be monitored.
17. Online safety (e-Safety) will be included in the PSHE, RSE and Computing programmes of study, covering both safe school and home use.
18. Acceptable use expectations and posters will be posted in rooms with Internet access.
19. Safe and responsible use of the internet and technology will be reinforced across the curriculum and within all subject areas.
20. The School will implement peer education to develop online safety as appropriate to the needs of the students as part of our on-line safety committee.

2.3 Awareness, education and training

2.3.1 Education of children and young people and young people considered to be vulnerable

The School is aware that all our students are vulnerable and that some may be considered to be even more vulnerable online due to a range of factors. The School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given.

2.3.2 Engagement and education of staff

1. The *Online Safety Policy* will be reinforced and highlighted as part of our safeguarding responsibilities and all staff are made aware of our *Acceptable Use of IT Policy – Staff* as part of induction procedures.
2. Staff will be made aware that our internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential when using School systems and devices.
3. Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on an annual basis as part of safeguarding training.
4. All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within the School. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

2.3.3 Engagement and education of parents and carers

1. The School recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and digital technology.
2. Parents' attention will be drawn to the school *Online Safety Policy* via the School website and the new student pack.
3. Information and guidance for parents on online safety will be made available to parents in regular 'E-safety advisor' newsletters on our web-site.

2.4 Security

2.4.1 Security and leadership of information systems

1. The security of the School information systems and users will be reviewed regularly.
2. Virus protection will be updated regularly.
3. Personal student data sent over the internet will be encrypted or accessed via appropriate secure remote access systems.
4. Portable media is discouraged.
5. Unapproved software will not be allowed in work areas or attached to email.
6. The School's ICT consultants will review system capacity regularly.
7. The appropriate use of user logins and passwords to access the School network will be enforced for all users.
8. All users will be expected to log off or lock their screens/devices if systems are unattended by using the Windows+L keyboard shortcut.

2.4.2 Password policy

1. All users will be informed not to share passwords or information with others and not to login as another user at any time.
2. Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
3. All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
4. Staff are issued with passwords to access School systems. If staff are given the opportunity to choose their own passwords for specific websites, they should ensure that they are unique passwords that contain a mix of upper- and lower-case letters, numbers and special characters. Staff should not use the same passwords for multiple websites and for School and personal use. Staff will use two-factor authentication (2FA) as directed.

2.4.3 Filtering and Monitoring

1. The School will ensure that the School has age- and ability-appropriate filtering and monitoring in place whilst using School devices and systems to limit children and young people's exposure to online risks.
2. The School's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students.
3. All users will be informed that use of School systems can be monitored.
4. The School uses filtering systems (Smoothwall) which block sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc. and alert staff to misuse of the School systems, the use of unsuitable language in their searches and work, and allow teachers to control their students' access to the internet or other sources of information during lesson times.
5. If staff or students discover unsuitable sites, the URL must be reported to the DSL and will then be recorded and escalated as appropriate.
6. SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
7. Any material that the School believes is illegal will be reported to appropriate agencies such as the Internet Watch Foundation (IWF), Kent Police or the Child Exploitation and Online Protection Centre (CEOP) immediately.

3 Responding, reporting and recording incidents

3.1 Responding to online incidents and safeguarding concerns

1. All members of the School community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying, etc. This will be highlighted within staff training and educational approaches for students.
2. All members of the School community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content, etc.
3. The DSL will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
4. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children and Young People Board thresholds and procedures.

5. Complaints about internet misuse will be dealt with under the School's complaints procedure.
6. Complaints about online/cyber bullying will be dealt with under the School's *Anti-Bullying Policy*.
7. Any complaint about staff misuse will be referred to the Headteacher.
8. Any allegations against a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).
9. Students, parents and staff will be informed of the School's complaints procedure.
10. Staff will be informed of the complaints and whistleblowing procedures.
11. All members of the School community will need to be aware of the importance of confidentiality and the need to follow the official School procedures for reporting concerns using My Concern.
12. The School will manage online safety (e-Safety) incidents in accordance with the School disciplinary procedures and *Behaviour Policy* where appropriate.
13. The School will inform parents/carers of any incidents of concerns as and when required.
14. After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes as required.
15. Where there is cause for concern or fear that illegal activity has taken place or is taking place, the School will contact the Education Safeguarding Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm.
16. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
17. If the School is unsure how to proceed with any incidents of concern, the incident will be escalated to the Education Safeguarding Team.
18. Parents and children and young people will need to work in partnership with the School to resolve issues.

3.2 Procedures for responding to specific online incidents or concerns

3.2.1 Responding to concerns regarding youth produced sexual imagery or "Sexting" and sharing nudes and semi-nudes

1. The School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting" and "sharing nudes and semi-nudes").
2. The School will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
3. The School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.
4. The School will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance KCSE 2016.

If the School are made aware of incident involving creating youth produced sexual imagery, the School will:

5. Act in accordance with the School's *Child Protection Policy* and *Safeguarding Policy* and the relevant Kent Safeguarding Child Board procedures.
6. Immediately notify the DSL. Staff must not ask the child/children or young person(s) involved in the incident to disclose information regarding the imagery. This is the

responsibility of the DSL. (Refer to the UK Council for Internet Safety document *Sharing nudes and semi-nudes: how to respond to an incident*.)

7. Store the device securely.
8. Carry out a risk assessment in relation to the children and young people(s) involved.
9. Consider the vulnerabilities of children and young people involved (including carrying out relevant checks with other agencies). Staff must not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers. (Refer to the UK Council for Internet Safety document *Sharing nudes and semi-nudes: how to respond to an incident*.)
10. Not say or do anything to blame or shame any young people involved.
11. Explain to anyone involved the need to report the incident and reassure them that they will receive support and help from the DSL. (Refer to the UK Council for Internet Safety document *Sharing nudes and semi-nudes: how to respond to an incident*.) The DSL will make a referral to the Police, if necessary.
12. Put the necessary safeguards in place for children and young people, e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
13. Implement appropriate sanctions in accordance with the School *Behaviour Policy* but taking care not to further traumatise victims where possible.
14. Review the handling of any incidents to ensure that the School is implementing best practice and SLT will review and update any leadership procedures where necessary.
15. The School will not view any images suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the DSL). Members of staff must never view, copy, print, share, store or save the imagery themselves, or ask a child to share or download it – this is illegal. If a member of staff has already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report to the DSL and seek support. (Refer to the UK Council for Internet Safety document *Sharing nudes and semi-nudes: how to respond to an incident*.)
16. Members of staff must not delete the imagery or ask a young person to delete it.
17. The School will not send, share or save content suspected to be an indecent image of children and young people and will not allow or request children and young people to do so.
18. If an indecent image has been taken or shared on the School network or devices, the School will act to block access to all users and isolate the image.
19. The School will act regarding creating youth produced sexual imagery, regardless of the use of School equipment or personal equipment, both on and off the premises.
20. The School will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

3.2.2 Responding to concerns regarding online child sexual abuse and exploitation

1. The School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and young people and how to respond to concerns.
2. The School will implement preventative approaches for online child sexual abuse via a range of age- and ability-appropriate educational approaches for students, staff and parents/carers.
3. The School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

4. If the School is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
5. If the School is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.

If the School are made aware of an incident involving online child sexual abuse of a child, the School will:

6. Act in accordance with the School's *Child Protection Policy* and *Safeguarding Policy* and the relevant Kent Safeguarding Child Board procedures.
7. Immediately notify the DSL.
8. Store any devices involved securely.
9. Immediately inform Kent Police via 101 (using 999 if a child is at immediate risk).
10. Where appropriate, the School will involve and empower children and young people to report concerns regarding online child sexual abuse, e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
11. Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
12. Make a referral to children and young people's social care (if needed/appropriate).
13. Put the necessary safeguards in place for student(s), e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
14. Inform parents/carers about the incident and how it is being managed.
15. Review the handling of any incidents to ensure that the School is implementing best practice and SLT will review and update any leadership procedures where necessary.
16. The School will act regarding online child sexual abuse regardless of the use of School equipment or personal equipment, both on and off the school premises.
17. The School will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
18. If students at other schools are believed to have been targeted, the School will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguard their community.

3.2.3 Responding to concerns regarding indecent images of children and young people

1. The School will ensure that all members of the community are made aware of the criminal nature of indecent images of children and young people including the possible consequences.
2. The School will take appropriate action regarding indecent images of children and young people regardless of the use of School equipment or personal equipment, both on and off the premises.
3. The School will act to prevent accidental access to indecent images of children and young people by implementing appropriate web filtering, implementing firewalls and anti-spam software.
4. If the School is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

If the School is made aware of indecent images of children and young people, the school will:

5. Act in accordance with the School *Child Protection Policy* and *Safeguarding Policy* and the relevant Kent Safeguarding Child Board procedures.
6. Immediately notify the DSL.
7. Store any devices involved securely.
8. Immediately inform appropriate organisations, e.g. the IWF, Kent Police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).

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

9. Ensure that the DSL is informed.
10. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk.
11. Ensure that any copies that exist of the image, for example in emails, are deleted.

If the School is made aware that indecent images of children and young people have been found on the School's electronic devices, the School will:

12. Ensure that the DSL is informed.
13. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk.
14. Ensure that any copies that exist of the image, for example in emails, are deleted.
15. Inform the Police via 101 (999 if there is an immediate risk of harm) and children and young people's social services (as appropriate).
16. Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the Police.

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

17. Ensure that the DSL is informed, or another member of staff in accordance with the School whistleblowing procedure.
18. Contact the Police regarding the images and quarantine any devices involved until Police advice has been sought.
19. Inform the LADO and other relevant organisations in accordance with the *School Managing Allegations against Staff Policy*.
20. Follow the appropriate School policies regarding conduct.

3.2.4 Responding to concerns regarding radicalisation and extremism online

1. The School will take all reasonable precautions to ensure that children and young people are safe from terrorist and extremist material when accessing the internet in School and that suitable filtering is in place which meets the needs of students.
2. When concerns are noted by staff that a child may be at risk of radicalisation online, the DSL will be informed immediately and action will be taken in line with the School *Safeguarding Policy*.
3. Online hate content directed towards or posted by specific members of the community will be responded to in line with existing School policies. If the School is unclear if a criminal

offence has been committed, the DSL will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.
4. All staff undertake *Prevent* training.
5. All students are taught about *Prevent* as part of their PSHE curriculum (as well as in other subjects, as appropriate).

3.2.5 Responding to concerns regarding cyberbullying

1. Cyberbullying, along with all other forms of bullying, of any member of the School community, will not be tolerated.
2. All incidents of online bullying reported will be recorded.
3. There are clear procedures in place to investigate incidents or allegations and support anyone in the School community affected by online bullying.
4. If the School is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
5. Students, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
6. The School will take steps to identify the bully where possible and appropriate. This may include examining School system logs, identifying and interviewing possible witnesses, and contacting the service provider and the Police, if necessary.
7. Students, staff and parents/carers will be required to work with the School to support the approach to cyberbullying and the School's ethos.

Sanctions for those involved in online or cyberbullying may include:

1. Those involved will be asked to remove any material deemed to be inappropriate or offensive.
2. A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
3. Internet access may be suspended at School for the user for a period of time. Other sanctions for students and staff may also be used in accordance with the School's *Anti-Bullying Policy*, *Behaviour Policy* and/or *Acceptable Use of IT Policies*.
4. Parent/carers of students involved in online bullying will be informed.
5. The Police will be contacted if a criminal offence is suspected.

3.2.6 Responding to concerns regarding online hate

1. Online hate will not be tolerated at the School. Further details are set out in the School *Anti-Bullying Policy* and *Behaviour Policy*.
2. All incidents of online hate reported to the School will be recorded.
3. All members of the community will be advised to report online hate in accordance with relevant School policies and procedures, e.g. the *Anti-Bullying Policy*, *Behaviour Policy*, etc.
4. The Police will be contacted if a criminal offence is suspected. If the School is unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
5. On-line hate is covered in the School's *Prevent* training (for staff) and lesson content (for students).

4 Links and resources (checked February 2023)

4.1 Online Safety (e-Safety) Contacts and References

www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

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

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children and young people Board (KSCB): www.kscb.org.uk

Kent e–Safety Blog: www.kentesafety.wordpress.com

EiS - ICT Support for Schools and Kent Schools' Broadband Service Desk: www.eiskent.co.uk

4.2 National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

NSPCC: https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Think U Know: www.thinkuknow.co.uk

UK Safer Internet Centre: www.saferinternet.org.uk

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