Online Safety Policy

The Sittingbourne School

Approved by:	Lynn Lawrence	**Date:** November 2023
Last reviewed on:	November 2023	
Next review due by:	November 2024	

Contents

Introduction

Online safety is an essential part of safeguarding. The internet and technology-based devices are an essential part of everyday life and students should be empowered to build resilience and to develop strategies to manage and respond to risk online. The Sittingbourne School believes that online safety is an integral part of safeguarding and acknowledges its role to ensure that all students and staff are protected from any harm that may arise online.

The Designated Safeguarding Lead at The Sittingbourne School is Mr A Campbell.

1. Aims

The purpose of this police is to:

- Safeguard and protect all members of the school online.
- Identify approaches to educate and raise awareness of online safety.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

Issues classified within online safety may be considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and
- non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing working group.

2. Policy Scope

The Sittingbourne School believes that online safety is an essential part of safeguarding. The Sittingbourne School identifies that the internet and associated devices (computers, tablets, mobiles) are an important part of everyday life. We believe that students should be empowered to build resilience and to develop strategies to manage and respond to risk appropriately online. This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers. This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as work laptops, tablets or mobile phones.

2.1 Policy links:

- Anti-bullying protocols.
- Acceptable use agreement for staff and for students.
- Child protection and safeguarding policy
- Values education.
- Personal development activities
- Mobile phone policy
- Procedures for reporting welfare concerns to a designated safeguarding lead

3. Monitoring and review

This policy and information report will be reviewed by the Designated Safeguarding Lead and Headteacher every year. It will also be updated if any changes to the information are made during the year.

Interest usage is closely monitored with any issues or concerns raised immediately by the filtering system to the Designated Safeguarding Lead immediately. To ensure they have oversight of online safety, the Head of School will be informed of online safety concerns, as appropriate. The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes. Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and responsibilities

The Designated Safeguarding Lead has overall responsibility for online safety. However, all members of the school play an important role with regards to online safety. Acceptable use agreements are included in staff safeguarding training and the process for reporting concerns is the same as any other safeguarding issue. There is open dialogue between the IT manager and the Designated Safeguarding Lead to ensure that online safety has the prominence it requires. The acceptable use agreement is comprehensive and should be read alongside this protocol. The agreement includes: social media use; email expectations; use of personal devices and communication.

4.1 Leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which cover acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfill their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this within the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the management team and to the safeguarding governor through regular meetings.

4.3 It is the responsibility of all members of staff to:

- Read and adhere to the online safety protocol and acceptable use protocols.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Staff personal mobile phones should not be used whilst involved in professional duties such as teaching or on duty.

- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support internally and externally.
- Take personal responsibility for professional development in this area.
- To support students to read and understand the student's acceptable use statement in a way which suits their age and ability.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety and procedures.
- Implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

4.5 It is the responsibility of students to:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the school acceptable use statement.
- Education and engagement with students
- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst students by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in relevant programmes of study.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching students to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - Training and engagement with staff

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use procedure and encourage their children to adhere to them.
- Role model safe online behaviour.
- Seek support and guidance from the setting or other agencies if there are risks or concerns online about their child/children.
- Be aware of changes in behaviour which could indicate that their child is at risk of

harm online.

- Abide by the acceptable use agreement.
- Support the school's approach to online safety and encourage and support safe online behaviour.

5. Education and engagement approaches

5.1 Education and engagement with learners:

The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Character Education and Sex Education (RSE) and computing programmes of study.
- Ensuring Personal Development Time provides ample opportunity for students to discuss Online Safety and develop an awareness of societal trends, issues and concerns
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable learners

The Sittingbourne School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

The Sittingbourne School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners: Targeted intervention groups responding to smoothwall, outcomes differentiated in lessons.

When implementing an appropriate online safety policy and curriculum The Sittingbourne School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - ➔ Educare online safety training CPD
    - ➔ Safeguarding briefings on online safety
    - ➔ Updates with reading and information
    - ➔ This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

The Sittingbourne School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing risks online

The Sittingbourne School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

7. Safer use of technology

7.1 Classroom use

We use a wide range of technology that include: computers/laptops, internet which may include search engines and educational websites, school learning platforms - Google Classroom, email, digital cameras, webcams and video cameras. All school owned devices will be used in accordance with the school's acceptable use agreement and with appropriate safety and security measures in place.
Members of staff will always evaluate websites, tools and apps fully and discuss their use with the DSL before use in the classroom or recommending for use at home if they are concerned.

The Sittingbourne School will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

- Google Safe Search or CBBC safe search.

We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledges the source of information.
The supervision of learners will be appropriate to their age and ability.

- Key Stage 3, 4, 5 learners will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and monitoring

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

- The school uses broadband connectivity through Wave9.
- The school uses Lightspeed which blocks sites that can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school works with Swale Academies Trust to ensure that our filtering policy is continually reviewed.
- Other sites may also be filtered out following a risk assessment by the DSL and the IT manager.

Dealing with filtering breeches

- The school has a clear procedure for reporting filtering breaches.
- If students discover unsuitable sites, they are encouraged to tell a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
- Parents/carers will be informed of filtering breaches involving their child that are a safeguarding concern.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: CSS, Kent Police or CEOP.

7.4 Managing personal data online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation and current Swale Data Protection Policy.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
    - ▪ Specific user logins and passwords will be enforced for all.
    - ▪ All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found at:
    - ▪ acceptable user policy

7.5.1 Password policy

● All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

● From year 7, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

● We require all users to:

- ➔ Use strong passwords for access into our system.
- ➔ Always keep their password private; users must not share it with others or leave it where others can find it.
- ➔ Not to login as another user at any time

Any questionable usage will be reported to the DSL and further action and support will be put in place for the student depending on need.

7.6 Managing the Safety of our Website

● We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

● We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

● Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

● The administrator account for our website will be secured with an appropriately strong password.

● We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

● We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

● Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

- o Spam or junk mail will be blocked and reported to the email provider.
- o Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

o Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

● Members of the community will immediately inform the Designated Safeguarding Lead if they receive offensive communication, and this will be recorded in our safeguarding files/records.

● Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

● We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff. Although all concerns are completed now via Bromcom.

7.8.1 Staff email

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

o All members of staff are provided with an email address to use for all official communication.

● Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

● Learners will use provided email accounts for educational purposes.

● Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Management of Learning Platforms

● The Sittingbourne School uses Google Classroom as its official learning platform.

● Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.

● Only current members of staff, learners and parents will have access to the LP.

● When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.

● Learners and staff will be advised about acceptable conduct and use when using the LP.

● All users will be mindful of copyright and will only upload appropriate content onto the LP.

● Any concerns about content on the LP will be recorded and dealt with in the following ways:

- o The user will be asked to remove any material deemed to be inappropriate or offensive.
- o If the user does not comply, the material will be removed by the site administrator.
- o Access to the LP for the user may be suspended.
- o The user will need to discuss the issues with a member of leadership before reinstatement.
- o A learner's parents/carers may be informed.
- o If the content is illegal, we will respond in line with existing child protection procedures.

● Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.

● A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.10 Management of Applications (apps) used to Record Children's Progress

● We use Bromcom to track learners progress and share appropriate information with parents and carers.

● The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

● To safeguard learner's data:

- ➔ Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- ➔ Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- ➔ Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- ➔ All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- ➔ Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Sittingbourne School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of The Sittingbourne School community are expected to engage in social media in a positive, safe and responsible manner.
- All members of The Sittingbourne 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.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
  - o The use of social media during setting hours for personal use is not permitted.
  - o Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of The Sittingbourne School community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Staff Personal Use of Social Media

- 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.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy. Reputation
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - o Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media. Advice will be provided to staff via staff training and by sharing appropriate guidance/resources on a regular basis. This will include (but is not limited to):

- o Setting the privacy levels of their personal sites.
- o Being aware of location sharing services.
- o Opting out of public listings on social networking sites.
- o Logging out of accounts after use.
- o Keeping passwords safe and confidential.
- o Ensuring staff do not represent their personal views as that of the setting.

● Members of staff are encouraged not to identify themselves as employees of The Sittingbourne School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.

● All members of staff are encouraged to carefully consider 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 our policies and the wider professional and legal framework.

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

● Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role. Communicating with learners and parents and carers

● All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.

- o Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Headteacher.
- o If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.

● Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the headteacher/manager.

● Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).

8.3 Learners' Personal Use of Social Media

● Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.

● We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.

● Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

  o Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

● Learners will be advised:

  o To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.

  o To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

  o Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.

  o To use safe passwords.

  o To use social media sites which are appropriate for their age and abilities.

  o How to block and report unwanted communications.

  o How to report concerns both within the setting and externally

8.4 Official Use of Social Media

● The Sittingbourne School official social media channels are:

  o Facebook

● The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

  o The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.

  o Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

● Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

  o Staff use setting provided email addresses to register for and manage any official social media channels.

  o Official social media sites are suitably protected and, where possible, run or linked from our website.

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

● Official social media use will be conducted in line with existing policies, including anti bullying, image/camera use, data protection, confidentiality and child protection.

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

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

o Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

o Any official social media activity involving learners will be moderated where possible.

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

● We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations:

● Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

● If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

o Sign our social media acceptable use policy.

o Always be professional and aware they are an ambassador for the setting.

o Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the setting.

o Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.

o Always act within the legal frameworks they would adhere to within the workplace including libel, defamation, confidentiality, copyright, data protection and equalities laws.

o Ensure that they have appropriate consent before sharing images on the official social media channel.

o Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.

o Not engage with any direct or private messaging with current, or past, learners, parents and carers.

o Inform their line manager, the DSL (or deputies) and the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of personal devices and mobile phones

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

9.1 Expectations

● All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.

● Electronic devices of any kind that are brought onto site are the responsibility of the user.

- o All members of The Sittingbourne School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- o All members of The Sittingbourne School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- o Mobile phones and personal devices are not permitted to be used.
- o The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- o All members of The Sittingbourne School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

● Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

● Staff will be advised to:

- o Keep mobile phones and personal devices in a safe and secure place during lesson time.
- o Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- o Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.

o Not use personal devices during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances.

o Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

● Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.

o Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) and Headteacher.

● Staff will not use personal devices:

o To take photos or videos of learners and will only use work-provided equipment for this purpose.

o Directly with learners and will only use work-provided equipment during lessons or educational activities.

● If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy o If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or has committed a criminal offence, the police will be contacted.

9.3 Learners' Use of Personal Devices and Mobile Phones

● Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

● The Sittingbourne School expects learners' personal devices and mobile phones to be kept out of sight at all times, other than designated times of day, such as break or lunch.

● If a learner needs to contact his/her parents or carers they will be allowed to use a setting phone.

o Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

● Mobile phones or personal devices will not be used by learners during lessons or formal educational time

o If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Headteacher or the Leadership Team

● Mobile phones and personal devices must not be taken into examinations. Learners 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 withdrawal from either that examination or all examinations.

● If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.

o Staff may confiscate a learner's mobile phone or device if they believe it is

being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).

o Searches of mobile phone or personal devices will only be carried out in accordance with our policy.
(www.gov.uk/government/publications/searching-screening-andconfiscation)

o Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
(www.gov.uk/government/publications/searching-screening-and-confiscation)

o Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.

o If there is suspicion that material on a learner'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.

9.4 Visitors' Use of Personal Devices and Mobile Phones

● Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

● We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

● Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Headteacher regarding any breaches of our policy.

9.5 Officially provided mobile phones and devices

● Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.

● Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

● Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to online safety incidents and concerns

● All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

● All members of the community must respect confidentiality and the need to follow the

official procedures for reporting concerns.

- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

● We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

● After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

● Safeguarding concerns and incidents should be reported to Digital Front Door, where appropriate.

● If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from CEOP or further agencies if required.

● Where there is suspicion that illegal activity has taken place, we will contact the Kent Police using 101, or 999 if there is immediate danger or risk of harm.

● If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Headteacher will speak with Kent Police to ensure that potential investigations are not compromised.

10.1 Concerns about Learners' Welfare

● The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.

  o The DSL (or deputies) will record these issues in line with our child protection policy.

● The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies.

● We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

● Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy.

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

● Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for responding to online safety incidents and concerns Social Media

● Our setting has accessed and understood sexual violence and sexual harassment between children in schools and colleges guidance (KCSiE, 2023)

● The Sittingbourne School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

● Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

● The Sittingbourne School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

● The Sittingbourne School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

● The Sittingbourne School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Character Education, RSE and Personal Develpment Time curriculum.

● We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

● We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

● If made aware of online sexual violence and sexual harassment, we will:

  o Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

  o If content is contained on learners' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

  o Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.

  o Implement appropriate sanctions in accordance with our behaviour policy. Inform parents and carers, if appropriate, about the incident and how it is being managed.

  o If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.

  o If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

o If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.

o Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

● The Sittingbourne School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

● We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.

● The Sittingbourne School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

● We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

● We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using school or personal equipment.

● We will not:

o 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 (if it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

o Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

● If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

o Act in accordance with our child protection policies

o Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

o Store the device securely.

o If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

o Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.

o Inform parents and carers, if appropriate, about the incident and how it is being managed.

o Make a referral to Children's Social Care and/or the Police, as appropriate.

o Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

o Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

o Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

o Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

o Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

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

● The Sittingbourne School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

● We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

● We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

● We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community on our website.

● If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

o Act in accordance with our child protection policies.

o If appropriate, store any devices involved securely.

o Make a referral to Children's Social Care (if required/appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)

o Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).

o Inform parents/carers about the incident and how it is being managed.

o Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

o Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

● We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

o Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

● If it is unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.

● If learners at other settings are believed to have been targeted, the DSL (or deputy) will seek support from the Police first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

● The Sittingbourne School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

● We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

● We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

● If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.

● If made aware of IIOC, we will:

o Act in accordance with our child protection policy

o Store any devices involved securely.

o Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.

● If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

o Ensure that the DSL (or deputy DSL) is informed.

o Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

o Ensure that any copies that exist of the image, for example in emails, are

deleted.

o Report concerns, as appropriate to parents and carers.

● If made aware that indecent images of children have been found on the setting provided devices, we will:

o Ensure that the DSL (or deputy DSL) is informed.

o Ensure that the URLs (web page addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

o Ensure that any copies that exist of the image, for example in emails, are deleted.

o Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).

o Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

o Report concerns, as appropriate to parents and carers.

● If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

o Ensure that the Headteacher is informed in line with our managing allegations against staff policy.

o Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.

o Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

● Cyberbullying, along with all other forms of bullying, will not be tolerated at The Sittingbourne School.

● Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online Hate

● Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Sittingbourne School and will be responded to in line with existing policies, including anti-bullying and behaviour.

● All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

● The Police will be contacted if a criminal offence is suspected.

● If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through Kent Police.

11.7 Online Radicalisation and Extremism

● We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

● If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.

● If we are concerned that a member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policy.

12.Useful Links for Educational Settings Kent Support and Guidance:

● Swale Education Safeguarding Service

  o Call: 03000 418 503

● If you are concerned about a child in Kent contact the Front Door on 03000 411111 or Frontdoor@kent.gov.uk

● Kent Safeguarding Children Multi-Agency Partnership 03000 421126 kscmp@kent.gov.uk

Kent Support and Guidance for Educational Settings

● https://www.kelsi.org.uk/child-protection-and-safeguarding

● https://www.theeducationpeople.org/our-expertise/safeguarding/

Kent Police:

www.kent.police.uk For non-urgent police contact 101 If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

● CEOP:

  o www.thinkuknow.co.uk

  o www.ceop.police.uk

● Childnet: www.childnet.com

● Internet Matters: www.internetmatters.org

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

● Lucy Faithfull Foundation: www.lucyfaithfull.org

● NSPCC: www.nspcc.org.uk/onlinesafety

  o ChildLine: www.childline.org.uk

- Net Aware: www.net-aware.org.uk

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk