Our school is a beacon of light. A place where every child and adult is encouraged to shine brightly and reach their full potential. Through curiosity, courage, and compassion, we shine like a lamp in our classrooms, like a village on a hill in our community, and like shining stars across the wider world.

Stelling Minnis CE Primary School

Online Safety Policy

Ratified: 9th June 2026

Reviewed Annually

1. Policy Aims

The purpose of Stelling Minnis CEP School's online safety policy is to:

- Safeguard and protect all members of the school community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- 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.

Stelling Minnis CEP School reocgnises the huge benefits of technology to the education of our pupils and to preparing them for future life. However, we identify that there are issues classified within online safety and ensuring that our pupils are safe online and that these can be broadly categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commercial: risks such as online gambling, scams, phishing, financial exploitation

2. Policy Scope

Stelling Minnis CEP School believes that online safety is an essential part of safeguarding and acknowledges our duty to ensure that all pupils and staff are protected from potential harm online. We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

We believe that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk 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 school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop, tablets or mobile phones.

3. Monitoring and Review

Stelling Minnis CEP School will review this policy every year. The policy will also be revised following any national or local policy requirements; any child protection concerns or any changes to the technical infrastructure. We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied. To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate. The named governor for safeguarding will report on a regular basis to the Full Governing Body on online safety incidents, including outcomes. Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

The Headteacher and DSL, has the overall responsibility for online safety, supported by the deputy DSLs. Stelling Minnis CEP School recognises that all members of the community have important roles and responsibilities to play with regards to online safety, including students.

The 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 the AUP.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Ensure they have sufficient time and resources dedicated to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school 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.

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 with 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.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Governing Body and appropriate agencies.
- Review and update online safety policies on a regular basis with stakeholder input.
- Discuss any E-safety related incidents/concerns with the governor with a lead responsibility for safeguarding/online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the e-safety policy and AUP policies.
- 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.
- 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.

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 policies 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.

It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

5. Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the Acceptable Use Policy and adhere to it.

6. Education and Engagement Approaches

Education and engagement with pupils

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 pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PSHE, RSE or Computing programmes of study, covering use both at home school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Vulnerable Pupils

Stelling Minnis CEP School is aware that some pupils are considered to be 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. We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. Stelling Minnis CEP School will seek input from specialist staff as appropriate, including the SENCO.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy 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 based on latest KCSIE guidance
- This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users/IP addresses; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.

- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with parents and carers

Stelling Minnis CEP School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school 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, newsletters and communications.
- Drawing their attention to the school e-safety policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.

7. Reducing Online Risks

Stelling Minnis CEP 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 school 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 a school computer or device.
- All members of the school community are made aware of the school's 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. This is clearly outlined in the AUP and highlighted through a variety of education and training approaches.

8. Safer Use of Technology Classroom Use

Stelling Minnis CEP School uses a wide range of technology. This includes access to:

- Computers, laptops, iPads and other digital devices
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- The school will use age appropriate search tools, following an informed risk assessment, to identify which tool best suits the needs of our community. The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Filtering and Monitoring

The governing body and school leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks. The governing body and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

Filtering

The school uses Schools Broadband supported by our IT provider SNS. The school uses the Netsweeper filtering system which blocks sites which can be categorised as: pornography, racial hatred, violence, extremism, gaming, advertising and sites of an illegal nature. The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list. The school works with Schools Broadband to ensure that our filtering policy is continually reviewed overseen by the designated Safeguarding Leads. See Child Protection policy for further information: Child Protection Policy (www.stelling-minnis.kent.sch.uk)

Dealing with Filtering breaches

The school has a clear procedure for reporting filtering breaches. If pupils discover unsuitable sites, they will be required to report this to a staff member immediately. 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 in the first instance. The breach will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child. Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 2018 and UK GDPR regulations. Full information can be found in the school's Data Protection Policy: Data Protection Policy.

Security and Management of Information Systems

The school takes 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 the school's network, The appropriate use of user logins and passwords to access the school network.
- Specific user logins and passwords will be enforced for all but the youngest users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Passwords

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. Pupils are responsible for keeping their usernames and passwords for educational platforms 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.

Managing the Safety of the School Website

The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). The school 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 pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number. The administrator account for the school website will be secured with an appropriately strong password. The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Publishing Images and Videos Online

The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): Staff Code of Conduct and Child Protection.

Managing Email

Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, Safer Working Practice/AUP. Spam or junk mail will be blocked and reported to the email provider. School email addresses and other official contact details will not be used for setting up personal social media accounts. Members of the school community will immediately tell the Designated Safeguarding Lead if they receive offensive communication, and this will be recorded in the school 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 in school.

Educational use of Videoconferencing

Stelling Minnis CEP School recognises that videoconferencing can bring a wide range of learning benefits. All video conferencing will be switched off when not in use.

Staff

The use of personal email addresses by staff for any official school business is not permitted. All members of staff are provided with a specific school 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 and pupils and parents.

Users

Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities. Pupils will ask permission from a teacher before making or answering a videoconference call or message. Videoconferencing will be supervised appropriately, according to the pupils' age and ability. Video conferencing will take place via official and approved communication channels following a robust risk assessment such as Zoom and Teams.

Only key administrators will be given access to videoconferencing administration areas or remote control pages. The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely. If third party materials are included, the school will check that recording is permitted to avoid infringing the third-party intellectual property rights. The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

9. Social Media

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Stelling Minnis CEP School's 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 Stelling Minnis CEP School community are expected to engage in social media in a positive, safe and responsible manner, at all times. All members of Stelling Minnis CEP 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. The school will control pupil and staff access to social media whilst using school provided devices and systems on site. The use of social media 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. Concerns regarding the online conduct of any member of Stelling Minnis CEP School community on social media, should be reported to the school and will be managed in accordance with our Antibullying, Allegations against Staff, Behaviour and Child Protection policies.

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 the Safer Working Practice/AUP.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may 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. All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

This will include (but is not limited to):

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

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 school's policies and the wider professional and legal framework.

Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead/Headteacher.

Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age. Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address,

mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.

- To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present. To use safe passwords.
- To use social media sites which are appropriate for their age and abilities. How to block and report unwanted communications and report concerns both within school and externally.

Official Use of Social Media

Stelling Minnis CEP School's official social media channels include Instagram and Facebook. The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes. Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website. Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data protection, Confidentiality and Child Protection. All communication on official social media platforms will be clear, transparent and open to scrutiny. Consent will be obtained, as required.

10. Use of Personal Devices and Mobile Phones

Stelling Minnis CEP 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 school.

Expectations

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child Protection. Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. All members of Stelling Minnis CEP School's community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises. All members of the 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. Mobile phones and personal devices are not permitted to be used during lesson time or in front of pupils, unless approved by the Headteacher. The sending of abusive or inappropriate messages/ 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. All members of Stelling Minnis CEP School are 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 Behaviour or Child protection policies.

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 school policy and procedures, such as: Safer Working Practice/ Conduct/AUP, Confidentiality, Child protection, Data Protection.

Staff will be advised to:

Keep mobile phones and personal devices in a safe and secure place during lesson time.

Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.

Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.

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

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 unless via our school communication system such as Class Dojo or School email.

Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead/Headteacher.

Staff will not use personal devices, such as: mobile phones, tablets or cameras: to take photos or videos of pupils and will only use work-provided equipment for this purpose/ directly with pupils, and will only use work-provided equipment during lessons/educational activities. The headteacher is exempt from this for the purposes of maintaining the school's Social Media accounts.

If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy.

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.

Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. Stelling Minnis CEP School does not permit pupils to being mobile phones or communication devices to school. Personal devices and mobile phones need to be handed into the school office or class teacher. They are then to be collected after school. If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Headteacher.

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 the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour and Child protection. Members of staff are expected to challenge

visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

Officially provided mobile phones and devices.

Members of staff may be issued with a work phone number and email address, where contact with pupils or parents/ carers is required (e.g. Wrap around care). School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff. School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies.

11. Responding to Online Safety Incidents and Concerns

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

All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns. Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure. The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team. Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or 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 the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Staff Misuse

Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations Against Staff/Whistleblowing 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 the Behaviour policy and KCSP Staff Code of conduct. Low level concerns should be reported to the DSL/HT.

12. Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery including "Sexting" or "upskirting" or AI generated Deep fakes

Stelling Minnis CEP School recognises youth produced sexual imagery (known as "sexting" or "upskirting") as a safeguarding issue; as well as the risk of images being created using Artificial Intelligence. Therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead. The school 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' as well as statutory guidance the latest KCSIE guidance (Keeping Children Safe in Education). Stelling Minnis CEP School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' and 'upskirting; by implementing preventative approaches, via a range of age and ability appropriate educational methods. The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with 'Sexting' or 'Upskirting'

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

- Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Specialist Children's Services and/or the Police, as appropriate.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with the school's behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the school 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.
- 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.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- 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 this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

Stelling Minnis CEP School will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers. The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally. The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community.

Dealing with Online Child Sexual Abuse and Exploitation

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

- Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store any devices involved securely.
- Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Make a referral to Specialist Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.

The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment. Where possible pupils 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 the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police. 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 Designated Safeguarding Lead. If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

Stelling Minnis CEP School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site. The school will take action 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 the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.

If made aware of IIOC, the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding procedures.
- Immediately notify the school Designated Safeguarding Lead.
- Store any devices involved securely.
- 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 pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- 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.
- 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 school devices, the school will:
- Ensure that the Headteacher is informed.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Quarantine any devices until police advice has been sought.

<u>Cyberbullying</u>

Cyberbullying, along with all other forms of bullying, will not be tolerated at Stelling Minnis CEP School. Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy. To help prevent cyber-bullying (also referred to as online bullying), we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss online bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail). In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal,

inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Online Hate

Online hate content, directed towards or posted by, any members of the community will not be tolerated at Stelling Minnis CEP School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour. All members of the community will be advised to report online hate in accordance with relevant school policies and procedures. The Police will be contacted if a criminal offence is suspected. If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

Online Radicalisation and Extremism

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school. If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy. If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher and Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child Protection and Allegations policies.

13. Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or Assistant Headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the
- opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's behaviour policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

14. Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Stelling Minnis CEP School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. The school will treat any use of AI to bully pupils in line with our behaviour and anti-bullying policy. In addition, staff are made aware that AI may spread misinformation or support the bypassing of filtering tools or support conspiracy theories. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment and assess any AI tool being used.

Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

Guidance for Educational Settings:

- www.kelsi.org.uk/support-for-children-and-young-people/child-protectionand-safeguarding
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
- Kent e–Safety Blog: www.kentesafety.wordpress.com

Kent Police

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

Other

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk