Sussex Road CP School
Online Safety Policy

Aims

This online safety policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2022, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures https://www.kscmp.org.uk/

This policy links with several other policies, practices and action plans, including, but not limited to:

- Child Protection Policy and Procedure
- Acceptable Use Policies (AUP) and the Code of Conduct
- Behaviour Policy
- Confidentiality Policy
- Data Management Policy
- Mobile phone Policy

The purpose of this online safety policy is to

- safeguard and promote the welfare of all members of Sussex Road School's community online
- identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns

Sussex Road School identifies that the issues classified within online safety are considerable but 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.

Scope

The School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online. As a school we acknowledge that the use of technology presents challenges and risks to children and adults both inside and outside of school. Sussex Road will empower, protect and educate the community in their use of technology and establish mechanisms to identify, intervene in, and escalate any incident where appropriate.

We identify that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.

We will empower our pupils to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

This policy applies to all staff, including the governing body, leadership team, 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 pupils and parents and carers.

This policy applies to all access to the internet and use of technology, including mobile technology, or where pupils, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

Key Contacts	**Name**	**Contact information**
Designated Safeguarding Lead (DSL) (Headteacher)	Mrs S Miles	Headteacher@sussex-road.kent.sch.uk 01732 352367 EX 206
Deputy Designated Safeguarding Lead	Mrs C Birkett	cbirkett@sussex-road.kent.sch.uk 01732 352367 EX 224
Deputy Designated Safeguarding Lead	Ms A Flaherty	aflaherty@sussex-road.kent.sch.uk 01732 352367 EX 224
SENCo	Ms A Flaherty	aflaherty@sussex-road.kent.sch.uk 01732 352367 EX 224
Chair of Governors and Safeguarding Governor	Mr M Webber	mwebber@sussex-road.kent.sch.uk

Monitoring and review

Technology evolves and changes rapidly; therefore, this policy will be reviewed annually, and revised following any national or local policy updates, any local child protection concerns and/or any changes to the school's technical infrastructure.

- Internet use will be supervised by staff as appropriate to pupils/students age and ability.
- Pupils/students will be directed to use age/ability appropriate online resources and tools by staff.
- Pupils/students will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessments.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of E-Safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

Roles and Responsibilities

The Designated Safeguarding Lead (DSL) is recognised as holding overall lead responsibility for online safety. However, all members of the community have important roles and responsibilities to play with regards to online safety. Our leadership team and relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with ICT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all pupils to develop an appropriate understanding of online safety.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as the Network Manager ICT Networks and the SENCO on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online.
- Ensure all members of staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and child protection training.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- 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 settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the school's SLT and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Report on E-Safety to the governor safeguarding team as part of their regular Monitoring Visits

It is the responsibility of all members of staff to:

- Online safety training for all school staff will be integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning. Staff are required to attend Online training in addition to annual Safeguarding Training.
- We recognise the expertise staff build by undertaking safeguarding training and from managing safeguarding concerns on a daily basis and staff are encouraged to contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our IT systems as well as staff and pupils and the electronic data they use or have access to.
- Model good practice when using technology with pupils
- Maintain a professional level of conduct in their personal use of technology, both on and off site in accordance with the school's Acceptable Use Policy and Staff Code of Conduct.
- 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 pupils in their care.
- Identify online safety concerns and take appropriate action by following the School safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers 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 the SLT, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures including as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide the School Usage Statement within the Admission Booklets.
- Seek help and support from the School or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety, by raising concerns with the school .as soon as any new concern or threat is detected by them.
- Use any School ICT systems, safely and appropriately. This includes the School's Twitter Feed and any Facebook page with clear links to the Sussex Road School Community.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

Education and engagement approaches

Education and engagement with pupils

The setting will establish and embed a whole School culture and will raise awareness and promote safe and responsible internet use amongst pupils by:

- ensuring our curriculum and whole School approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
- ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study
- reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site
- implementing appropriate peer education approaches as necessary
- creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
- involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content.
- making informed decisions to ensure that any educational resources used are appropriate for our pupils.
- using external visitors, where appropriate, to complement and support our internal online safety education approaches. *Using External Visitors to Support Online Safety Education: Guidance for Educational Settings*
- providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.

The School will support pupils to understand and follow our Acceptable Use policy in a way which suits their age and ability by:

- displaying acceptable use posters in all rooms with internet access.
- informing pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
- seeking pupil voice when writing and developing online safety policies and practices, including curriculum development and implementation.

We will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:

- ensuring age-appropriate education regarding safe and responsible use precedes internet access.
- teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
- educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
- enabling them to understand what acceptable and unacceptable online behaviour looks like.
- preparing them to identify possible online risks and make informed decisions about how to act and respond.
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Pupils

The School recognises that any pupil can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.

We will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable pupils.

Staff at Sussex Road School will seek input from specialist staff as appropriate, including the DSL, SENCO, Child in Care Designated Teacher to ensure that the policy and curriculum is appropriate to our community's needs.

Training and engagement with staff

We will

- require all new staff members to confirm they have read the School's Safeguarding policies including this E-Safety Policy and the most up to date Keeping Children Safe in Education document as part of the appointment process
- provide annual up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach.
- require all staff to read the regular LEA Child protection Newsletters

Staff training covers the potential risks posed to pupils (content, contact and conduct) as well as our professional practice expectations.

- build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff could use with pupils.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.

Awareness and engagement with parents and carers

We recognise 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
- drawing their attention to our online safety policy and other external communication (such as letters and social media channels) as well as on our website and the School's Twitter feed
- requesting parents and carers read online safety information as part of joining our community and sign the Online statement within the School's admission booklet
- requesting parents and carers read online safety information annually and sign the Online statement within the School's Home School Planner.

Reducing Online Risks

The 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 their use in the School is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.

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. This is clearly outlined in our Acceptable Use Policy and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom use

We use a wide range of technology. This includes access to:

- Computers, laptops, tablets and other digital devices
- Internet, which may include search engines and educational websites
- Learning platform/intranet
- Email
- Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies 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 setting will use appropriate search tools as identified following an informed risk assessment.

The children's homepage is set to Swiggle.org.uk - Child Friendly Search Engine for Kids friendly search. They can use google but Bing is blocked completely

We 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 internet access and technology use will be appropriate to pupils age and ability.

Early Years Foundation Stage and Key Stage 1

Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils age and ability.

Key Stage 2

Pupils will use age-appropriate search engines and online tools such as Swiggle.org.uk - Child Friendly Search Engine for Kids

Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils age and ability.

We will balance children's ability to take part in age-appropriate activities online, with the need to detect and prevent abuse, bullying or unsafe practice in accordance with the National Minimum Standards (NMS).

Managing internet access

We will maintain a data base of users who are granted access to our devices and systems.

All staff, pupils and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

Filtering and monitoring

Leaders and DSLs access the guidance for education settings about establishing 'appropriate levels' of filtering and monitoring to help inform their decision making: www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Decision making

Sussex Road School leaders have ensured that our School has age and ability appropriate filtering and monitoring in place to limit pupil's exposure to online risks.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

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.

The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.

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.

Appropriate filtering

Sussex Road School's education broadband connectivity is provided through the KPSN (Kent Public Service Network).

We use Smoothwall filtering.

Smoothwall blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

Smoothwall is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC). *Leaders should check to ensure this is the case.*

Smoothwall integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office' *Leaders should check to ensure this is the case.*

We work with KPSN to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

If pupils or staff discover unsuitable sites or material, they are required to turn off monitor/screen, report the concern immediately to a member of SLT, who will report the URL of the site to the ICT Administrator and EIS.

Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving pupils.

Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

Appropriate monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

Detail how this may be achieved by physical monitoring (supervision), monitoring internet and web access (reviewing log file information) and/or active/pro-active technology monitoring services. Where required Leaders and DSLs will also access www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring for further information about appropriate monitoring approaches and what they entail.

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

If a concern is identified via monitoring approaches we will:

List how concerns will be responded to e.g., DSL or deputy will respond in line with the child protection policy.

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.

Full information can be found in our information security policy which can be accessed at (*Link or location*).

Password policy

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

We require all users to

- use strong passwords for access into our system.
- change their passwords every month.
- not share passwords or login information with others or leave passwords/login details where others can find them.
- not to login as another user at any time.
- lock access to devices/systems when not in use.

All pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.

Managing the safety of our website

We will ensure that information posted on our website meets the requirements as identified by the 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 pupil’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.

Publishing images and videos online

We will ensure that all images and videos shared online are used in accordance with the School's Data Management policy and GDPR regulations, Acceptable Use policy, Codes of Conduct and mobile phones policy.

Managing email

Access to our email systems will always take place in accordance with GDPR legislation and in-line with policies, including Confidentiality, Acceptable Use of Policy and the Code of Conduct.

The forwarding of any chain messages/emails is not permitted.

Spam or junk mail will be blocked and if appropriate reported to the EIS/LEA.

Setting email addresses and other official contact details will not be used to set up personal social media accounts.

All Members of the community will immediately tell a member of SLT if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Staff email

All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.

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

Pupil email

Pupils will use a provided with an internal email account for educational purposes enabling the ICT curriculum to be fully taught. Pupils will receive education regarding safe and appropriate email etiquette before access is permitted. Where concerns are raised regarding the content of Pupil internal emails the school reserves the right to access the content of messages sent.

Iris Connect

The School uses Iris Connect to enable teachers to record lessons for self, or peer monitoring and review. Such recordings are held securely online and accessible only to the originator or invited colleagues. Where concerns are raised regarding the content of recordings the school reserves the right to access the content.

On occasion the system is used to record specific pupil's behaviour or educational needs providing evidence to families and external agencies. These records are kept in accordance with the School's GPDR and Data management policy.

Social Media

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of the 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 community are expected to engage in social media in a positive and responsible manner.

All members of the community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

We will control pupil and staff access to social media whilst using the school's provided devices and systems on site.

The use of social media during School hours for personal use is only permitted to access information, posting comments and uploads are not permitted. For more information regarding appropriate site please refer to the school's Acceptable Use Policy. Personal devices may be used to search for information requested by pupils as part of a lesson where the school's device may not be easily available. The process must however be carried out by the staff member and at no point should the devices be handed to the pupils to search or access the results. Inappropriate or excessive use of social media during school hours or whilst using School devices may result in removal of internet access and/or disciplinary or legal action.

Uploads to the School's social media (Twitter Feed) may only be undertaken by the Headteacher.

The use of social media is not permitted in school for pupils.

Concerns regarding the online conduct of any member of the Sussex Road School community on social media, will be reported to the DSL and be managed in accordance with our safeguarding policies.

All staff will be made aware of the professional risks associated with the use of social media and electronic communication (such as email, mobile phones, texting, social networking). Staff will adhere to relevant Sussex Road policies including staff behaviour policy, Acceptable Use Policies, and Social Media

Pupils 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.

We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. Any concerns regarding pupils use of social media will be dealt with in accordance with existing policies. Concerns regarding pupil's use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Pupils will be advised:

- to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
- to only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so 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.
- how to report concerns on social media, both within the setting and externally.

Official use of social media

The School's official social media channels is Twitter @Sussexroad. The official use of social media sites by the School only takes place with clear educational or community engagement objectives and with specific intended outcomes.

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

The Headteacher has 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 accounts for official educational or engagement purposes only.

Official social media use will be conducted in line with existing policies. All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.

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.

The School acknowledges that the PTA (SRSA) operate a Facebook page and retain the right for inappropriate/incorrect post to be removed by the moderator.

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.

The school's expectation regarding pupils' personal devices and mobile phones is dealt with in the School's mobile phones policy.

Mobile phones or personal devices will not be used by pupils during the school day and parents are advised to contact their child via the School Office during the school day, rather than a pupil's personal device. If a pupil breaches the policy, the phone or device will be confiscated and held in a secure place. Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy. Mobile phones and devices that have been confiscated will be released to parents/ carers.

If there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Responding to Online Safety Incidents

All members of the community will be made aware of the CPOMS reporting procedure for concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.

All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.

Pupils, 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 pupils to work in partnership with us to resolve online safety issues.

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

If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Service.

Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.

If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL or Headteacher will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

Concerns about pupil online behaviour and/or welfare

The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.

All concerns about pupils will be recorded in line with our child protection policy.

The School recognises that whilst risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.

The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

Appropriate sanctions and/or pastoral/welfare support will be offered to pupils as appropriate. Civil or legal action will be taken if necessary.

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

Concerns about parent/carer online behaviour and/or welfare

Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher and/or DSL (or deputy). The Headteacher and/or DSL will respond to concerns in line with existing policies.

Civil or legal action will be taken if necessary.

Welfare support will be offered to parents/carers as appropriate.

Procedures for Responding to Specific Online Concerns

Online sexual violence and sexual harassment between children

The Headteacher, DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.

The school may also seek additional support from *www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals*

Full details of our response to peer-on-peer abuse, including sexual violence and harassment can be found in our Safeguarding and Child Protection policy.

The 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
- 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

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 any concerns relating to online sexual violence and sexual harassment, we will:

- immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- if content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy.
- inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
- if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

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

We recognise that 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.

We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, we 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.

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

Youth produced sexual imagery ("sexting")

The School recognises youth produced sexual imagery (also 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 UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local KSCMP guidance: "Responding to youth produced sexual imagery".

Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.

It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery 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 the taking and sharing of youth produced sexual imagery. We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.

If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.

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

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

- act in accordance with our child protection policies and the relevant local procedures.
- ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance.
- store any devices containing potential youth produced sexual imagery securely

If content is contained on pupil's personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

If a potentially 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.

- carry out a risk assessment in line with the UKCIS and KSCMP guidance which considers the age and vulnerability of pupils involved, including the possibility of carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and KSCMP guidance.
- provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

- consider the deletion of images in accordance with the UKCIS guidance.

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.

- 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.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

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

We will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target pupils, and understand how to respond to concerns.

We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils, staff and parents/carers.

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

We will ensure that the ‘Click CEOP’ report button used to report online child sexual abuse is visible and available to pupils and other members of our community.

If made aware of an incident involving online child abuse and/or exploitation, we will:

- act in accordance with our child protection policies and the relevant KSCMP procedures.
- store any devices containing evidence securely.
- If content is contained on pupil’s personal devices, they will be managed in accordance with the DfE ‘searching screening and confiscation’ advice.
- If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
- if appropriate, make a referral to Children’s Social Work Service and inform the police via 101, or 999 if a pupil 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 and provide support and signposting, as 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; leadership team will review and update any management procedures, where necessary.

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

Where possible and appropriate, pupils will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).

If members of the public or pupils at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.

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 (IWF) 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 and/or the Education Safeguarding Service.

If made aware of IIOC, we will:

- act in accordance with our child protection policy and the relevant KSCMP procedures.
- store any devices involved securely.
- immediately inform appropriate organisations, such as the IWF and police.

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

- ensure that the DSL (or deputy) is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF 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 setting provided devices, we will:

- ensure that the DSL (or deputy) is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
- inform the police via 101 or 999 if there is an immediate risk of harm, and Children's Social Work Service, as appropriate.
- only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
- report concerns, as appropriate to parents/carers.

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

- ensure that the Headteacher is informed in line with our managing allegations against staff policy.
- inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.
- quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Sussex Road School.

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

Online hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at Sussex Road School and will be responded to in line with existing policies, including child protection, 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) will obtain advice through the Education Safeguarding Service and/or the police.

Online radicalisation and extremism

As listed in this policy, we will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. All staff members are required to complete radicalisation training as part of the appointment process

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

If we are concerned that 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 policies.

Where children are asked to learn online at home in response to a full or partial closure:

We will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements and any local/national guidance.

All communication with pupils and parents will take place using school provided or approved communication channels, for example, the school’s email and texting services, the school’s landlines and/or agreed systems e.g., Microsoft 365, Zoom or Tapestry.

Staff and pupils will engage with remote teaching and learning in line with existing behaviour principles as set out in our school Behaviour policy/Code of conduct and Acceptable Use Policies.

Staff and pupils will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

When delivering remote learning, the school will aim to ensure that pupils have reasonable opportunities to use digital technology to enhance their learning. All staff and pupils will be expected to be responsible users of digital technology in line with the expectations set out in the Acceptable Use Policy. This policy is available on the school web site.

Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. These sites include but are not limited to: Oak Academy, Whiterose and BBC Bitesize. The school will continue to be clear who from the school (if anyone) their child is going to be interacting with online.

Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

Children are asked to:

- be suitably dressed and ready to learn on zoom calls.
- be in a communal area within their house i.e., not the bedroom.
- have an adult within earshot of any live sessions.
- not use the chat function unless requested by the class teacher.
- unmute themselves when asked to by class teacher.
- show respect to their peers and adults when using zoom and other social media
- cooperate with others
- be friendly
- listen to others
- treat everyone with respect
- take responsibility for their own behaviour

Staff are required to:

- be aware of their background if teaching from home and to maintain a professional attitude.
- take a register of every zoom call and absences or safeguarding concerns followed up by class teacher and SLT, if child has not been present for three zoom calls.
- follow normal procedures for any safeguarding concerns resulting from remote learning.
- ensure equipment is used safely and for its intended purpose
- have good awareness of issues to do with safeguarding and child protection and take action when appropriate.
- model good behaviour for children to follow.
- challenge all unacceptable behaviour and report any breaches to SLT.
- ensure DSLs have the login details to any live sessions to complete drop ins when necessary

Other requests:

- laptop/dongle permission slips have been filled in for school devices that have been loaned out to families.
- cross reference with the Safeguarding policy.
- no one is permitted to record the live sessions without full consent from the HT.

Appendix A

Support Agency Contact details

Guidance for Educational Settings:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
www.theeducationpeople.org/blog/?tags=Online+Safety&page=1
KSCMP: www.kscb.org.uk

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 non-urgent enquiries, contact Kent Police via 101

Front Door:
The Front Door can be contacted on 03000 41 11 11
Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:
EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eisit.uk
National Links and Resources for Settings, Pupils and Parents/carers
CEOP:
www.thinkuknow.co.uk
www.ceop.police.uk

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

UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
Report Harmful Content: https://reportharmfulcontent.com/

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

Childnet: www.childnet.com
Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

Internet Matters: www.internetmatters.org

Parent Zone: https://parentzone.org.uk

Parent Info: https://parentinfo.org

NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

Action Fraud: www.actionfraud.police.uk

Get Safe Online: www.getsafeonline.org

Appendix B

Pupil Acceptable Use of Technology Statements

Although statements for pupils are collected within key stages, it is recommended that settings amend and adapt them according to their own cohorts needs. The template statements and headers are suggestions only and some statements are duplicated; we encourage educational settings to work with pupils and amend them to develop ownership and understanding.

Early Years and Key Stage 1 (0-6)

- I only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do
- I keep my personal information and passwords safe
- I only send messages online which are polite and friendly
- I know the School can see what I am doing online
- I always tell an adult/teacher/member of staff if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk (*include other appropriate links*) to learn more about keeping safe online
- I have read and talked about these rules with my parents/carers

Shortened version (for use on posters)

- I only go online with a grown up
- I am kind online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried

Key Stage 2 (7-11)

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate, and if I have permission
- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I use School computers for School work, unless I have permission otherwise
- I will not use my own personal devices/mobile phone in school
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher has allowed me to

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher
- I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I should not or that makes me feel worried or upset then I will minimise the page and tell an adult straight away *(amend to reflect your approach e.g., shut the laptop lid, turn off the screen*)

Shortened KS2 version (for use on posters)

- I ask a teacher about which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first
- I know that people online are strangers, and they may not always be who they say they are
- If someone online suggests meeting up, I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

Pupils with SEND functioning at Levels P4 –P7

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see anything that I don't like online, I tell a grown up

Pupils with SEND functioning at Levels P7-L1
(Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- On the internet I do not tell strangers my name

Meeting

- I tell a grown up if I want to talk on the internet

Accepting

- I do not open emails from strangers

Reliable

- I make good choices on the computer

Tell

- I use kind words on the internet
- If I see anything that I do not like online, I will tell a grown up

Pupils with SEND functioning at Levels L2-4 (Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online, I talk to an adult

Accepting

- I do not open messages from strangers
- I check web links to make sure they are safe

Reliable

- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online then I do not reply, I save the message and show an adult
- If I see anything online that I do not like, I will tell a teacher

Appendix C

Internet usage agreement in planners

INTERNET USAGE

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.

· These rules will keep everyone safe and help us be fair to others.

· I will tell my teacher immediately if I come across any information that makes me feel uncomfortable.

· I will only use my own or our class’s internet password.

· I will only send emails to people I know who have been approved by my class teacher.

· I will not give out personal information on the Internet such as my address, telephone number. Parent’s work address, telephone number, or the name of my school without permission from my teacher.

· I will never send a person a picture or anything else without first checking with my teacher.

· When I do send a message, I will ensure that it is polite and responsible.

· I will not respond to any messages that are mean or in any way make me feel uncomfortable.

· I will not bring any memory sticks, USB pen drives or other external storage systems into school for use on the school’s computer network system unless I have been given permission to do so.

· I understand that the school can and will check my files in order to monitor the Internet sites that I visit.

Please read and sign to confirm you have read the “Online and E-Safety policy” and “Online Safety” section on our website at www.sussex-road.kent.sch.uk

I have read and discussed the above with my child.