"Learning Today, Leading Tomorrow"

Bishops Down Primary and Nursery School

www.bishopsdownprimary.org

Online Safety Policy

Reviewed by	HT & FGB
Date approved	28 March 2022
Date of next review	Spring 2023
Policy reference	Kent Model

Policy Aims

Bishops Down Primary & Nursery School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones' and/or 'smart watches')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

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

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation
- Early years foundation stage (EYFS) statutory framework - GOV.UK (www.gov.uk)
- Working together to safeguard children - GOV.UK (www.gov.uk)
- Procedures - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk)

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act

2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

Links with other policies and practices
This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and Staff Code of Conduct
- Behaviour policy
- Child protection policy
- GDPR Policy
- Privacy Notice
- Image use policy

Monitoring and Review
Technology evolves and changes rapidly; as such Bishops Down Primary and Nursery School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

Roles & Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

Ensure that they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Leadership Team

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Leadership 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; including an acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and that they work with technical staff to monitor the safety and security of our systems and networks.
- 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.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners 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 learners to develop an appropriate understanding of online safety.

The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- In ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- 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 learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners 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.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

- Contribute to the development of our online safety policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- 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 learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Take personal responsibility for professional development in this area.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

Notify a member of staff or the head teacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

- 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.
- Abide by the 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 setting, or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of the online safety policies.
- Use systems, such as Purple Mash safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet International

Parent resource sheet – Childnet International

Healthy relationships – Disrespect Nobody

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 terms on acceptable use.

Education and Engagement Approaches

Education and engagement with learners

Bishops Down Primary and Nursery School will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners 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 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.
- creating a safe environment in which all learners 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 learners who may be impacted by the content.
- making informed decisions to ensure that any educational resources used are appropriate for our learners.
- 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.
- rewarding positive use of technology.

Bishops Down Primary and Nursery School will ensure learners 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 learners 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 Learners

As a school with a Special Resource Provision (SRP) for children with physical disabilities and complex medical needs, Bishops Down Primary and Nursery School recognises that some children rely heavily on the digital world to support their developing social needs. We also recognise that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, 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. Bishops Down Primary and Nursery School will ensure that differentiated and ability appropriate

online safety education, access and support is provided to vulnerable learners. Staff at Bishops Down Primary and Nursery School will seek input from specialist staff as appropriate, including the DSL, SENDCo to ensure that the policy and curriculum is appropriate to our community's needs.

Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This takes place at the first INSET day of the school year and a register kept.
- Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
- build on existing expertise by providing 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 learners.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

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

We will build a partnership approach to online safety with parents and carers by providing information and guidance on online safety in a variety of formats

- Through the website, newsletter or on email
- requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
- requiring them to read our acceptable use policies and discuss the implications with their children.

<u>Reducing Online Risks</u>

Bishops Down Primary and Nursery School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks.

- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the 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.
- 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 computers 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 to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

Bishops Down Primary and Nursery School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- iPads
- 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. There is no access to settings on tablets so changes cannot be made to the core of the tablet. Bishops Down Apple ID is locked in.
All laptops and other mobile devices remain in school unless signed out and authorised by IT Manager / Head teacher. If iPads are taken off site a lock-screen function will be enabled prior to this occurring.
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 age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. Some of these search tools include, Google Safe Search, CBBC Safe Search, Swiggle, DKImages SWGfL Squiggle, Dorling Kindersley Find Out, www.primaryschoolict.com, www.bbc.co.uk, www.kdrex.org.
We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

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

Key Stage 2

Learners will use age-appropriate search engines and online tools and will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Managing Internet Access

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

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

Bishops Down Primary and Nursery School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks. The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what 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 learners; effective classroom management and regular education about safe and responsible use is essential.

Appropriate Filtering

Bishops Down Primary and Nursery School's broadband connectivity is provided through Cantium. Bishops Down Primary and Nursery School uses Smoothwall. 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).

Smoothwall integrates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

We work with Cantium to ensure that our filtering policy is continually reviewed. If learners discover unsuitable sites, they will be required to:

- turn off monitor/screen only and report the concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

-

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by physical monitoring (supervision), monitoring internet and web access (reviewing logfile information). An email is sent to the Headteacher and IT technician if access has been sought to blocked content. We refer to www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring for further information.

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:

- Immediately inform the DSL or in her absence one of the deputies.
- The DSL will then follow relevant safeguarding procedures according to the school 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 GDPR policy on the school website).

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network. Children are not expected to use passwords to access the school network whilst in school, but they do have passwords linked to their Microsoft Teams accounts.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private. Pupils requires passwords only to access Microsoft Teams and Purple Mash.

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.
- lock access to devices/systems when not in use.

Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

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

The administrator account for our website will be secured with an appropriately strong password. We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: image use, GDPR, acceptable use policies, code of conduct.

Managing Email

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

The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider. Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email or attachments will be suitably password protected.

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

Members of the community will immediately tell Clare Owen, Head teacher if they receive offensive communication, and this will be recorded in our safeguarding files/records. Excessive social email use can

interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site. We will have a dedicated online reporting system (CPOMS) for reporting wellbeing and pastoral issues. This is managed by designated and trained staff.

Staff email

The use of personal email addresses by staff for any official setting business is not permitted. All members of staff are provided with an email address to use for all official communication. Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents. Staff should not reply to parents after 6pm and should use the office@ email to forward messages to parents.

Management of Learning Platforms

Bishops Down Primary and Nursery School uses Microsoft Teams as its official learning platform. Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities. Only current members of staff will have access to the LP. When staff leave the setting, their account will be disabled or transferred to their new establishment. All users will be mindful of copyright and will only upload appropriate content onto the LP. Any concerns about content on the LP will be recorded and dealt with in the following ways:

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

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

We use Tapestry to track learners progress and share appropriate information with parents and carers of Nursery and Early Years pupils. We use Target Tracker to record progress of children from years 1-6. Some children with special educational needs have their progress tracked using BSquared. The Head teacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data

- only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.

- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Social Media

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Bishops Down Primary and Nursery 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 Bishops Down Primary and Nursery School community are expected to engage in social media in a positive and responsible manner. All members of Bishops Down Primary and Nursery School 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 learner and staff access to social media whilst using school provided devices and systems on site by the use of Smoothwall. The use of social media during school hours for personal use is not permitted for staff. The use of social media during school hours for personal use is not permitted for learners. 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.

Concerns regarding the online conduct of any member of Bishops Down Primary and Nursery School community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, 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 our code of conduct and acceptable use of technology policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media 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 appropriate privacy levels on their personal accounts/sites.
- Being aware of the implications of using location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Using strong passwords.
- Ensuring staff do not represent their personal views as being that of the setting.

Members of staff are encouraged not to identify themselves as employees of Bishops Down Primary and Nursery School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members. All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites. Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted. All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the Head teacher.

- Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.

If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools. Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

Learners Personal Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach via age appropriate sites and resources. We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.

Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

Learners 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

Bishops Down Primary and Nursery School official social media channels are Twitter, Instagram and Facebook. The official use of social media sites by Bishops Down Primary and Nursery 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 Head teacher. Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence. Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.

Staff use setting provided email addresses to register for and manage official social media channels. Official social media sites are suitably protected and are run and linked from our website. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague. Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.

All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community. Only social media tools, Twitter, Instagram and Facebook, which have been risk assessed and approved as suitable for educational purposes will be used.

Bishops Down primary & Nursery School also has a YouTube channel. Any videos that are uploaded to this channel are set to be privately listed and can only be accessed by people who have the specific link.

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required. We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

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

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

- Sign our social media acceptable use policy.
- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role but make it clear that they do not necessarily speak on behalf of the setting.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputy) of any concerns, such as criticism, inappropriate content or contact from learners.

Mobile Technology: Use of Personal Devices and Mobile Phones

Bishops Down Primary and Nursery School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

Expectations

All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.

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

- All members of Bishops Down Primary and Nursery School community are advised to take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of Bishops Down Primary and Nursery 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 in specific areas within the site such as changing rooms, toilets and swimming pools. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying and behaviour policies.

All members of Bishops Down Primary and Nursery School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

Staff Use of Personal Devices and Mobile Phones

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

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 needed to communicate via Microsoft Teams.
- 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 learners or parents and carers.

- Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy) and Head teacher.
- Staff will not use personal devices or mobile phones:
    - to take photos or videos of learners and will only use work-provided equipment for this purpose.
    - directly with learners and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our staff 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 using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Learners Use of Personal Devices and Mobile Phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences. Only children in Year 6 are permitted to bring a mobile phone into school. In some instances children in lower year groups may have specific permission from the Head teacher. Bishops Down Primary and Nursery School expects learners' personal devices and mobile phones to be switched off (unless needed for medical purposes). These devices need to remain in children's bags until the end of the school day. If a learner needs to contact his/her parents or carers they will be allowed to use the school office phone. Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.

Mobile phones or personal devices will not be used by learners during the school day or in Beehive (Wrap around Care). Mobile phones and personal devices must not be taken into examinations. Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations. If a learner breaches the policy, the phone or device will be confiscated and held in a secure place. Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy. Searches of mobile phone or personal devices will be carried out in accordance with the KCC policy, which is linked to DfE 'Searching, Screening and Confiscation' guidance. Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies in line with the DfE 'Searching, Screening and Confiscation' guidance. Mobile phones and devices that have been confiscated will be released to parents/ carers at the end of the day. If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors, including volunteers and contractors, should ensure that personal devices are not used within the school and grounds during the school day. Contractors needing to use their phones will be asked to make and receive calls in the front car park.

Appropriate signage and information is provided in the front entrance and on volunteers code of conduct advice sheet to inform parents/carers and visitors of expectations of use.

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use. Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) or Head teacher of any breaches of our policy.

Officially provided mobile phones and devices

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

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. Setting mobile phones are to be taken on off-site activities to prevent the need of staff using their own devices. Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

Responding to Online Safety Incidents and Concerns

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

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns. Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.

Where there is suspicion that illegal activity has taken place, we 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 our community (for example if other local settings are involved or the public may be at risk), the DSL will speak with Kent Police *and/or* the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Concerns about Learners Welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL (or deputy) will record these issues in line with our child protection policy.

All concerns about learners will be recorded on CPOMS in line with our child protection policy.

Bishops Down Primary and Nursery School recognises that whilst risks can be posed by unknown individuals or adults online, learners 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 learners 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 staff online behaviour and/or welfare

Any complaint about staff misuse will be referred to the Head teacher, in accordance with our allegations against staff policy. Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer). Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff behaviour policy and code of conduct. Welfare support will be offered to staff as appropriate.

Concerns about parent/carer online behaviour and/or welfare

Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Head teacher and/or DSL (or deputy). The Head teacher and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.

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 Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children
The Head teacher and DSLs access Childnet's online sexual harassment guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals for advice and guidance.
Our Head teacher, DSLs and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2021 guidance and 'Keeping children safe in education' 2021. Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.

Bishops Down Primary and Nursery 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 learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- provide the necessary safeguards and support for all learners 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.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Bishops Down Primary and Nursery School recognises 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.

Bishops Down Primary and Nursery School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

To help minimise concerns, Bishops Down Primary and Nursery School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online

sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.

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

Youth Produced Sexual Imagery ("Sexting")

Bishops Down Primary and Nursery School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB 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.

Bishops Down Primary and Nursery School 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 and through our RSE provision.

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. Documents can be found in the staffroom. 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 learners 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 learners 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 learners 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 learners, 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)

Bishops Down Primary and Nursery 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.

Bishops Down Primary and Nursery School 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 learners, 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 learners, staff and parents/carers. Use of NSPCC posters, online safety assemblies.

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.

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 learners 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 learner is at immediate risk.
- carry out a risk assessment which considers any vulnerabilities of learner(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 learners, 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, learners 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 learners 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)

Bishops Down Primary and Nursery School 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 learner 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 Bishops Down Primary 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 Bishops Down Primary and Nursery School and will be responded to in line with existing policies, including anti-bullying and behaviour. All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.

Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) 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 Head teacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings

Education Safeguarding Team:

- 03000 415797
    - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
    - Ashley Assiter, Online Safety Development Officer
- 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.kscmp.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, Learners 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