Online Safety Policy

The Folkestone School for Girls Academy Trust is known as "the school" in this policy.

Policy Aims

This policy has been written by The Folkestone School for Girls involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, 'Working Together to Safeguard Children' 2018 and the Kent Safeguarding Children Board procedures.

It is essential that children are safeguarded from potentially harmful and inappropriate online material and behaviours. An effective approach to online safety enables educational settings to empower, protect and educate learners and staff in their use of technology and establishes mechanisms to identify, intervene and escalate any concerns where appropriate.

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

The school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk, as per KCSIE:

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

However, we assert that there is a fifth **C**, **Culture**. It is inescapable that students and young people use technology as a fundamental part of their wider culture and they communicate and are connected almost 24/7. This shapes a large part of who they are and how they are, both as individuals and as a community. As per our safeguarding policy, we see the greatest challenges to keeping students safe as being in their own mental health and well-being and we feel that a large part of that concern and deterioration comes from our online lives. We must therefore seek to educate students, not just in terms of their own online safety as indicated through the 4 Cs but on the toll that our online life can have on our real life. There are wider issues to consider; screen time and over connection, FOMO, issues such as fake news and the misinformation and disinformation so common online. Fake news is more than just deep fakes; nor does

it always relate to 'news'. It is believing all that is said in chats and by peers as gospel. Indeed, as part of our Global Education 'One World' curriculum and as part of our cross-curricular projects, students study an entire unit on whether or not we can really believe what we see, hear and read via media anymore. We use the fascinating story of 'The Shed at Dulwich' to capture their interest! But more than just believing what we see and read, from 'the news' to other websites through to deep fakes there is a fundamental concern as to how students also believe all that their peers write; there is equally a concern as to how we conduct ourselves online, not just in terms of causing harm, but just in terms of our general manners; saying things online that we would never say face-to-face. A separate project also looks at immigration and some of the misleading information that feeds and fuels extremist ideology.

This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches, most notably as part of our PSHE curriculum which is delivered in discrete lessons across all year groups. FSG will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.

FSG recognises that technology and the risks and harms related to it, evolve, and change rapidly. Therefore this policy is reviewed bi-annually to consider these. 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.

The Principal will be informed of online safety concerns by the DSL, as appropriate. The named Trustee for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider board.

Policy Scope

The school believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. The school identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

The school believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the board of trustees, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

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

- Anti-bullying
- Staff Code of conduct
- Behaviour

- Staff discipline
- Safeguarding
- Confidentiality
- Relationship & Sex Education (RSHE)
- GDPR
- Whole School Equality
- SRE

Monitoring and Review

Technology, and risks and harms related to it, evolve and change rapidly. The school will review this policy at least annually.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the Principal will be informed of online safety concerns, as appropriate.

The named trustee for safeguarding will report on a regular basis to the board of trustees on online safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

Roles and Responsibilities

The Designated Safeguarding Lead (DSL) has lead responsibility for online safety.

The school recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy *or* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The DSL will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside the Deputy DSL to ensure online safety is recognised as part of the schools safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date 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.
- 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 schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the schools management team and board of trustees.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (*Bi-Annually*) with the Trustee responsible for safeguarding and online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the schools safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team (firewall, email filtering, school wide WIFI network for students and guidance to staff and students for email use) to ensure that the schools IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.

- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or Deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:
- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:
- Read the acceptable use 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.
- Abide by the home-school agreement and/or acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement Approaches

Education and engagement with learners:

The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
- ensuring education regarding safe and responsible use precedes internet access.
- including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSHE) and computing programmes of study - and in particular, instruction with respect to peer-on-peer abuse, sexual harassment and the sharing of indecent images either consensually or non-consensually
- reinforcing online safety messages whenever technology or the internet is in use.
- educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
- displaying acceptable use posters in all rooms with internet access.
- informing learners that network and internet use will be monitored for safety and security purposes including email exchange and internet searches and in accordance with legislation.
- rewarding positive use of technology.

- implementing appropriate peer education approaches.
- providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Learners

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

The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

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

Training and engagement with staff

We will:
- provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
- staff will complete an annual safeguarding training programme, which covers online safety. The school will also provide guidance to staff on keeping themselves safe online and ask all staff to read *"Keeping Children Safe in Education 2021"* and *"what to do if you are worried a child is being abused"*.
- this will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- make staff aware that our IT systems are monitored, including email exchange and internet searches and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- make staff aware that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

Awareness and engagement with parents and carers
- the 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:
  o providing information and guidance on online safety in a variety of formats.

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

Reducing Online Risks and managing Mobile & Smart Technology

The school is currently in the process of phasing out mobile phone usage on site; this is a phased approach with each new year group. At present students in Years 7, 8, 9, 10 & 11 are no longer allowed access to phones whilst in school. They should be switched off and in bags/blazers. Sixth form students are able to access the school wi-fi to encourage its usage and thus to succumb to our school filtering systems.

Monitoring systems are also deployed to identify concerning internet searches.

Nonetheless it is impossible to ensure that students on the school site do not use their own devices to access content online and thus to ensure that any content is suitable. Instead, we must seek to educate students, not just in terms of their own online safety, but also in terms of wider issues such as fake news and the misinformation and disinformation so common online.

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 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, whilst acknowledging that given to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. 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 - The 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
- Learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

All school owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Entire site coverage for our WIFI network has been created so that students can access the internet safely with the school able to filter out content. Members of staff will

always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The school will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We should use search tools, which help filter content for staff and learners. Examples could include SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search. Our firewall will also filter searches and block sites identified as a risk.

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.

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

Learners in residential provision - We will balance children's ability to take part in age-appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

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

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Decision Making

The trustees and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

The trustees 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.

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.

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.

Filtering

Education broadband connectivity is provided through Virgin. We use Smoothwall to block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.

We work with Smoothwall to ensure that our filtering policy is continually reviewed. If learners discover unsuitable sites, they will be required to:
- turn off monitor/screen and report the concern immediate 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.

Student Blocked Categories

Legal and Liability
Child Abuse
Drugs
Intolerance
Piracy and Copyright
Pornography
Self-Harm
Terrorism
Violence

Adult Themes
Abortion
Adult entertainers
Adult Sites
Alcohol and Tobacco
Body Piercing and Tattoos
Criminal Activity
Fireworks
Gambling
Gore
Inappropriate Vulgar search terms
Naturism and Nudism
Nudity
Provocative Images
Restricted to Adults
Sexuality Sites

Weapons
Hunting and Sporting
Military
Personal Weapons

Files
Document Macros
Executable Files

Malware and Hacking
Hacking
Malware and Phishing
Web Proxies

Social Media
Blogs
Dating Sites
Discussion Forums
Facebook
Instant messaging Voip and Web
Conferencing
Social Networking Sites
Twitter

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 school owned or provided internet enabled devices. This is achieved by physical monitoring (supervision), monitoring internet and web access (including internet searches and trigger words and, for our escape room only, through CCTV.

Monitoring systems are deployed on all school machines to identify concerning internet searches or email exchanges surrounding key words. Such monitoring systems are successfully utilised though it should be noted that most searches that are flagged and investigated tend to be students 'messing around' rather than alert us to genuine safeguarding concerns. Nonetheless, reports to the Principal highlight smoothwall filtering alerts and nominated staff investigate should any unusual or unsuitable internet searches be made. The system does work well - highlighting, for instance, 2 recent searches by members of staff as they carried out research to support the construction of the 'bomb' for our escape room!

Similarly, in a recent safeguarding investigation, email exchanges between specific end users was easy to isolate to support the investigation process.

The challenge is to prevent access to damaging materials whilst not 'over blocking' to disrupt teaching and learning. In that vein then we can create **custom allowed lists** such that staff can inform us of specific websites that students will need access to and we can then open these; so for example criminology students will certainly want/need to research criminal activity online. By opening certain 'pre-checked' sites we can do this.

If a concern is identified via monitoring approaches t*he DSL or Deputy will respond in line with the safeguarding policy.*

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

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.

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:
- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all *but the youngest users.*
- 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 password to access our systems; members of staff are responsible for keeping their password private.

Since 2018, all learners are provided with their own unique username and private password to access our systems; learners are responsible for keeping their password private.

We require staff users to:
▪ use strong passwords for access into our system;
▪ change their passwords annually;
▪ 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.
▪ Not use the same password for school as for personal 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 student's personal information will not be published on our website; the contact details on the website will be our school 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 cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Managing Email

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

School 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 the DSL 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. This is monitored through the school systems and alerts created when the acceptable volume is exceeded. This is reported to the DSL for investigation.

Staff Email

The use of personal email addresses by staff for any official school 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 emails, especially if communication is taking place between staff, learners and parents and our staff code of conduct sets explicit parameters for such exchanges, including timings, frequency and length of individual exchanges.

Emailing Students

Electronic communication between students and adults should take place within clear and explicit professional boundaries and only via the school email system (or other agreed systems ie: Hegarty Maths etc.) which can be monitored by the school. Electronic communication may only be about matters related to school. Staff must not engage in long email exchanges with students and if after 4 emails the matter has not been resolved, the fifth email should be to suggest that the student comes to see you on the next working school day to resolve the matter. Staff are strongly encouraged to email students between 8am and 6pm on school days only. They should not exchange emails with students during weekends and holidays. Should a member of staff feel that it may be necessary to contact a student at a time other than those stated, they should first seek permission from a member of SLT.

Staff email addresses are generally not published on our school website. This is to discourage parents from contacting teachers directly. Of course, there may be instances when teachers will contact parents directly concerning student progress or wellbeing or other school matters, but these should be driven by the teacher. Staff should, as for students, avoid lengthy email exchanges with parents and avoid emailing outside the hours mentioned above. Staff should instead report to their line managers, when an email challenges their decision making ie: issuing detentions, awarding places for teams/casts etc.

Student Email

Students will use provided email accounts for educational purposes, will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

Educational use of Videoconferencing and/or Webcams

The school recognise that video conferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits. All video conferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.

Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.

Video conferencing contact details will not be posted publicly.

Video conferencing equipment will not be taken off the premises without prior permission from the DSL.

Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

Parents/carers consent will be obtained prior to learners taking part in video conferencing activities.
Learners will ask permission from a member of staff before making or answering a video conference call or message.
Video conferencing will be supervised appropriately, according to the learner's age and ability.
Video conferencing will take place via official and approved communication channels following a robust risk assessment.
Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

When recording a video conference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely. If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

Management of Learning Platforms

The school uses google classroom as its official learning platform (LP). Leaders and staff will regularly monitor the usage of the LP, including message/communication tools and publishing facilities.

Only current members of staff, students and parents will have access to the LP. When staff and/or students leave the school, their account will be disabled. Staff and students will be advised about acceptable conduct and use when using the LP. All users will be mindful of copyright and will only upload appropriate content onto the LP.

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

Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

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

We use SIMs Parent App to track learner's progress and share appropriate information with parents and carers. The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

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

Social Media - Expectations

The expectations' regarding safe and responsible use of social media applies to all members of the school community and are clearly laid out in our staff code of conduct.

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 school community are expected to engage in social media in a positive, safe and responsible manner.

All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control learner and staff access to social media whilst using devices provided by the school and systems on site.

The use of social media during school hours for personal use is not permitted. Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of the school community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff Personal Use of Social Media

School staff's social media profiles should not be available to students. If they have a personal profile on social media sites, they should not use their full name, as students may be able to find them. Staff should consider using a first and middle name instead and set public profiles to private.

The member of staff has a responsibility to understand the settings associated with their social media and use them to ensure their profile is private. Staff should also be clear that any opinions they express online are their own and are not affiliated to The Folkestone School for Girls. Indeed, it is our strong suggestion that staff do not advertise their position as a member of school staff on social media at all. Staff should also be aware that actions, images or views expressed online are also subject to the conditions laid out in **Part 2 of Teacher Standards.**

Staff should not attempt to contact students or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find students' or parents' social media profiles. Staff will ensure that they do not post any images online that identify children who are students at the school without their consent.

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 school and profession. 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 the privacy levels of their personal sites.
▪ being aware of location sharing services.
▪ opting out of public listings on social networking sites.
▪ logging out of accounts after use.
▪ keeping passwords safe and confidential.
▪ ensuring staff do not represent their personal views as that of the schools.

Members of staff are encouraged not to identify themselves as employees of The Folkestone School for Girls on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, 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 Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with Learners and Parents/Carers:

Personal contact details **should not** be exchanged between staff and students. This includes social media profiles.

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

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

Staff will not use personal social media accounts or email addresses to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Principal.

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 state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.

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

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

Learners will be advised:
- to consider the benefits and risks of sharing personal details 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 responsible adult's permission and only when a trusted adult is present.
- to use safe passwords.
- to use social media sites which are appropriate for their age and abilities.
- how to block and report unwanted communications.
- how to report concerns both within the school and externally.

Use of Personal Devices and Mobile Phones

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

The school is currently in the process of phasing out mobile phone usage on site; this is a phased approach with each new year group. Students in years 7, 8, 9, 10 & 11are no longer allowed access to phones whilst in school ; They should be switched off and in bags/blazers.

Sixth Form students are able to access the school wi-fi to encourage its usage and thus to succumb to our school filtering systems. Monitoring systems are also deployed to identify concerning internet searches.

Expectations:
- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- All members of the school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of the school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of the 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.
- 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. (There are some notable exceptions; in the case of an expectant parent who may well have their phone on 'standby' - see below)
  - not use personal devices during teaching periods, unless permission has been given by the Line Manager, such as in emergency circumstances.
  - ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - 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/or the Principal.
- staff will not use personal devices:
  - 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 code of conduct/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, the police will be contacted.

The school is a busy, buzzing and vibrant community and images of the countless trips and opportunities that we provide go far to promote, _internally_, our curriculum, our culture and our ethos. They demonstrate the variety of experiences on offer to girls and the 'whole child/every child' curriculum they benefit from.

They provide a 'day in the life' insight to parents who are increasingly remote from their child's lived experience in school **and** they provide a whole school overview to all staff as to the impact they have! Whilst we endeavour to use school cameras or phones where possible, such is the volume and array of activities on offer, that this is not always possible. Staff therefore may, on occasion, use their own personal devices to capture images. Any images recorded in this way should be uploaded to the school network or google drive as soon as is practically possible and deleted entirely from personal devices once uploaded.

Learners Use of Personal Devices and Mobile Phones:

- learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- the school expects learners' personal devices and mobile phones to be kept in a secure place, switched off, kept out of sight during throughout the school day - unless a teacher has given express permission to use the device.
- if a learner needs to contact her parents/carers they will be allowed to use a school phone or maybe given express permission to use their phone to do so. 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 SDL during lessons if appropriate.
- mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- mobile phones and personal devices, including watches must not be taken into examinations. Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- if a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - searches of mobile phone or personal devices will only be carried out in accordance with our policy - www.gov.uk/government/publications/searching-screening-and-confiscation for 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.
  - mobile phones and devices that have been confiscated will be released to parents or 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) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or Deputy) or Principal 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.
- School 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 schools are involved or the public may be at risk), the DSL or Principal 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. The DSL (or Deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures. We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

Any complaint about staff misuse will be referred to the Principal, in accordance with the allegations policy. Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer). Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children:

- our school has accessed and understood part 5 of 'Keeping children safe in education'
- the school recognises that sexual violence and sexual harassment between children can take place online. Examples may include; consensual and/or non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- the 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.
- the school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- the school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- we will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- we will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- if made aware of online sexual violence and sexual harassment, we will:
  - immediately notify the DSL (or Deputy) and act in accordance with our child protection and anti-bullying policies.
  - if content is contained on learner's electronic 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 offering specific advice on blocking, reporting and removing online content, as well as 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 a referral 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 establishment, 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 Kent 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.

Youth Produced Sexual Imagery ("Sexting"):
- the 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".
- the school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- we will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

- we will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site using school or personal equipment.
- we will not:
  - view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is deemed necessary, the image will only be viewed by the DSL (or Deputy) and their justification for viewing the image will be clearly documented.
  - send, share, save or make copies of content suspected to be an indecent image of 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 Kent Safeguarding Child Board's procedures.
  - ensure the DSL (or Deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Store the device securely.
- if an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
  - inform parents and carers, if appropriate, about the incident and how it is being managed.
  - make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' 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 UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' 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 Child Sexual Abuse and Exploitation (including child criminal exploitation):
- the school will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- the school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or Deputy).
- we will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- we will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- we will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.

If made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation) we will:
- act in accordance with our CP policies and the relevant Kent Safeguarding Child Board's procedures.

- if appropriate, store any devices involved securely.
- make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
- carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- inform parents/carers about the incident and how it is being managed.
- 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 child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment. Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns via the Click 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 Team and/or Kent 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 Child Sexual Exploitation Team (CSET) by the DSL (or Deputy).
- if learners at other schools are believed to have been targeted, the DSL (or Deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC):
- the school will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- we will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- we will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- if we are unclear if a criminal offence has been committed, the DSL (or Deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- if made aware of IIOC, we will:
  - act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
  - store any devices involved securely.
  - immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- if made aware that a member of staff or a 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 Internet Watch Foundation via www.iwf.org.uk .
  - ensure that any copies that exist of the image, for example in emails, are deleted.
  - report concerns, as appropriate to parents and carers.
- if made aware that indecent images of children have been found on school 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 Internet Watch Foundation via www.iwf.org.uk .
  - ensure that any copies that exist of the image, for example in emails, are deleted.

- o inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- o only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- o report concerns, as appropriate to parents and carers.
- if made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
  - o ensure that the Principal is informed in line with our managing allegations against staff policy.
  - o inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - o quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at the 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 the 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 a member of staff may be at risk of radicalisation online, the Principal will be informed immediately and action will be taken in line with the child protection and allegation policies.

Useful Links for Educational Settings - Kent Support and Guidance for Educational Settings
Education Safeguarding Team:
- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, Online Safety Development Officer - Tel: 03000 415797
- Guidance for Educational Settings:
  - o www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
  - o www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - o www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
  - o Kent Online Safety Blog: www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCB: - 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 other non-urgent enquiries contact Kent Police via 101

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

National Links and Resources for Educational Settings
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

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