

□



Online Safety Policy

Policy for	Online Safety
Persons Responsible	Lead DSL Mrs Emma Beal and Chair of Governors Mrs Anna Lawrence
Date Last Reviewed	October 2022
Date of Next Review	October 2023
Date Last Approved by Governors	
Date Next Approval by Governing Body	September 2023

	Name	Contact Information
Designated Safeguarding Lead (DSL)	Emma Beal	emma.beal@swale.at
Deputy Designated Safeguarding Lead	Nikki Ball Gina Adams Dawn Aldous	Nikki.ball@swale.at Gina.adams@swale.at Dawn.aldous@swale.at
Head of School	Lee Downey	Lee.downey@swale.at
Safeguarding Governor	Anna Lawrence	anna.lawrence@swale.at

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

The Holmesdale School Online Safety Policy

1. Policy Aims

- This online safety policy has been written by The Holmesdale school, 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](#)' 2022, '[Working Together to Safeguard Children](#)' 2018 and the local [Kent Safeguarding Children Multi-agency Partnership \(KSCMP\)](#) procedures.
- The purpose of THS online safety policy is to:
 - safeguard and promote the welfare of all members of the Holmesdale community online.
 - identify approaches to educate and raise awareness of online safety throughout our community.
 - enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - identify clear procedures to follow when responding to online safety concerns.
- The Holmesdale school identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk.
 - Content: being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
 - Contact: being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
 - Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
 - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

2. Policy scope

- The Holmesdale School recognises 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 Holmesdale School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.
- The Holmesdale school will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- This policy applies to all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners and parents and carers.

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

2.2 Links with other policies and practices

- This policy links with several other policies, practices, and action plans, including but not limited to:
 - Anti-bullying policy
 - Acceptable Use Policies for students and staff
 - The Holmesdale Staff Code of Conduct
 - Behaviour Policy
 - Child Protection Policy
 - Image Use
 - Mobile Technology and Social Media

3. Monitoring and review

- Technology evolves and changes rapidly; as such The Holmesdale 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.
- To ensure they have oversight of online safety, the Head of school will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding (Jayne Ingman) will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- The Holmesdale School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems. The IT Network Manager will ensure that appropriate filtering and monitoring systems are in place and liaise with the Lead DSL.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Mrs Emma Beal, is recognised as holding overall lead responsibility for online safety.
- The Holmesdale school recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a whole school culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, child on child abuse, use of social media and mobile technology.
- Work with IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.

- Support the DSL and the deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, 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 curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the school on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians, and the SENCO on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the school's safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep 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.
- 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 and school policies and procedures.
- Report online safety concerns, as appropriate, to the school senior leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

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

- Read and adhere to our online safety policy and acceptable use of technology 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 THS safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

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

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

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

4.6 It is the responsibility of parents and carers to:

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement.
- Seek help and support from the school or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The school will establish and embed a whole THS 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) guidance.
 - ensuring online safety is addressed in PSHE, and IT programmes of study.
 - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
 - implementing appropriate peer education approaches such as peer mentoring.
 - 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.
 - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
- The Holmesdale School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
 - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
 - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- The Holmesdale 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.

5.2 Vulnerable Learners

- The Holmesdale school recognises 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.
- The Holmesdale school will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.
- Staff at The Holmesdale school will seek input from specialist staff as appropriate, including the DSL and SENCO, to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will
 - provide and discuss the online safety policy and procedures with all members of staff as part of induction.
 - provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach. This will be achieved as part of the annual training and also by means of updates.
 - 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 provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.
 - make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
 - make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
 - highlight useful educational resources and tools which staff could use with 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.

5.4 Awareness and engagement with parents and carers

- The Holmesdale 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 through email and newsletters.
 - drawing their attention to our online safety policy and expectations in our newsletters and on our website.
 - 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.

6. Reducing Online Risks

- The Holmesdale School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
 - regularly review the methods used to identify, assess, and minimise online risks.
 - examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use in the school is permitted.
 - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
 - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- The Holmesdale School uses a wide range of technology. This includes access to:
 - Computers, laptops, tablets
 - Internet, which may include search engines and educational websites
 - Email
- All school devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use appropriate search tools as identified following an informed risk assessment.
- 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 internet access and technology use will be appropriate to learners age and ability.

7.2 Managing internet access

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

7.3 Filtering and monitoring

[Appropriate Filtering and Monitoring - UK Safer Internet Centre](#)

7.3.1 Decision making

- Holmesdale LGB 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.

- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The governors and leaders are mindful to ensure that “over blocking” does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate filtering

- Holmesdale uses Fortinet which 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.
- Fortinet is a member of [Internet Watch Foundation](#) (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
- Fortinet integrates the ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’
- We work with Fortinet and Imeria to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to report the concern immediately to a member of staff.
- Filtering breaches will be reported to the DSL (or deputies) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

7.3.3 Appropriate monitoring

- The school will appropriately monitor internet use on all school owned or provided internet-enabled devices. This is achieved by:
 - Physical monitoring, monitoring internet and web access.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. The DSL will respond in line with the Child Protection Policy.
- All users will be informed that use of the school system can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing personal data online

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

- Full information can be found in our GDPR policy.

7.5 Security and management of information systems We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- 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.
- Specific user logins and passwords will be enforced for all users.
- All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password Policy

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

- From year 7, all students are provided with their own unique username and private passwords to access school systems; students are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.
 - Change passwords regularly
 - Lock access to devices/systems when not in use.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner'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.

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the image use, acceptable use policies, codes of conduct/mobile technology/social media policies.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including the code of conduct.
- 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 to set up personal social media accounts.
- Members of the community will immediately tell Emma Beal if they receive offensive communication, and this will be recorded in our safeguarding files/records.

7.8.1 Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.8.2 Learner email

- Learners will use a provided email account for educational purposes.
- Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Holmesdale community.
- The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger.
- All members of the Holmesdale community are expected to engage in social media in a positive and responsible manner.
 - All members of the Holmesdale community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
 - The use of social media during school hours for personal use is not permitted for staff.
- Concerns regarding the online conduct of any member of the Holmesdale 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.

8.2 Staff personal use of social media

- The safe and responsible use of social media 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.

8.2.1 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.
 - 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 services. 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:
 - School 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 school.
- Members of staff are encouraged not to identify themselves as employees of The Holmesdale school on their personal social networking accounts; this is to prevent information 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. Staff are expected 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.

8.2.2 Communicating with learners and parents/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 DSL and the Head of school.
 - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the school and members of staff.
- 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 school provided communication tools.

- Any communication from learners and parents received on personal social media accounts will be reported to the DSL and the Head of school.

8.3 Learners' 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 school and externally.

8.4 Official use of social media

The Holmesdale School official social media channels are - Twitter; Facebook; Instagram

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Head of school.
 - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use school provided email addresses to register for and manage any official school social media channels.
 - Official social media sites are suitably protected.
 - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including Anti-bullying, data protection, child protection.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.

- Parents, carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
 - Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
 - Any official social media activity involving students will be moderated by the school where possible.
- Parents and carers will be informed of any official social media use with students and written parental consent will be obtained, as required.
- The school 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.

8.4.1 Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional 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 school, they will:
 - Sign our social media acceptable use policy.
 - Be aware they are an ambassador for the school.
 - Be professional, 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 appropriate consent has been given before sharing images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
 - Not engage with any private/direct messaging with current or past learners or parents/carers.
 - Inform the DSL (or deputies) and the Head of school of any concerns, such as criticism, inappropriate content or contact from learners.

9. Mobile Technology: Use of Personal Devices and Mobile Phones

- The Holmesdale 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 school.

9.1 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 the Holmesdale 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 The Holmesdale 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 owned by students are not permitted to be used during the school day (8.45am – 3.15pm).
- 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 The Holmesdale School are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff use of personal devices and mobile phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection, and acceptable use of technology.
- Staff will be advised to
 - keep mobile phones and personal devices in a safe and secure place such as a drawer 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.
 - 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 and/or the Head of school.
- 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.

9.3 Learners' use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
 - The Holmesdale School expects learners' personal devices and mobile phones to be switched off and kept out of sight whilst at school.
- If a learner needs to contact his/her parents or carers they will be allowed to use the office phone.
 - Parents are advised to contact their child via the office; exceptions may be permitted on a case-by-case basis, as approved by the Head of school.
- 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.
 - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
 - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.
 - Searches of mobile phone or personal devices will be carried out in accordance with our behaviour policy and 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.

9.4 Visitors' use of personal devices and mobile phones

- 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 of any breaches of our policy.

9.5 Officially provided mobile phones and devices

9.6 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 of technology policy and other relevant policies.

Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, child on child abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
 - 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 with us to resolve online safety issues.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Education Safeguarding Service.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about learner online behaviour and/or welfare

- The DSL (or deputies) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- The Holmesdale school recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputies) 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.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Head of school, 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 code of conduct.

- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Head of school. The Head of school will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, 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.

11. Procedures for Responding to Specific Online Concerns

11.1 Online sexual violence and sexual harassment between children

- The Head of School and the DSL 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 part 5 of 'Keeping Children Safe in Education' 2022
 - Full details of our response to child on child abuse, including sexual violence and harassment can be found in our child protection policy.
- The Holmesdale 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 deputies) 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 school, 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 deputies) 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.
- The Holmesdale 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 Holmesdale School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, The Holmesdale 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 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.

11.2 Youth produced sexual imagery (“sexting” and “sharing nudes and semi nudes”)

- The Holmesdale School recognises youth produced sexual imagery (also known as “sexting”) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputies).
- We will follow the advice as set out in the non-statutory UKCIS guidance: [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#), and the local [KSCMP](#) guidance: “Responding to youth produced sexual imagery”.
 - Youth produced sexual imagery or ‘sexting’ is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
 - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- The Holmesdale 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.
- 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 such as the staff room and safeguarding folder on the p drive.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school 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 deputies) 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.

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

- The Holmesdale 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 deputies), in line with our child protection policy.
- The Holmesdale 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.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community which can be found on the school website.
- 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 school 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 deputies) 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 schools are believed to have been targeted, the DSL (or deputies) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- The Holmesdale 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 deputies) 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 deputies) 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 school provided devices, we will:
 - ensure that the DSL (or deputies) 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 Head of school 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.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Holmesdale School
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Holmesdale School and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputies) will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, 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 learner or adult may be at risk of radicalisation online, the DSL (or deputies) 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 of school will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Responding to an Online Safety Concern Flowchart

Key Local Contacts

Designated Safeguarding Lead : Mrs E Beal

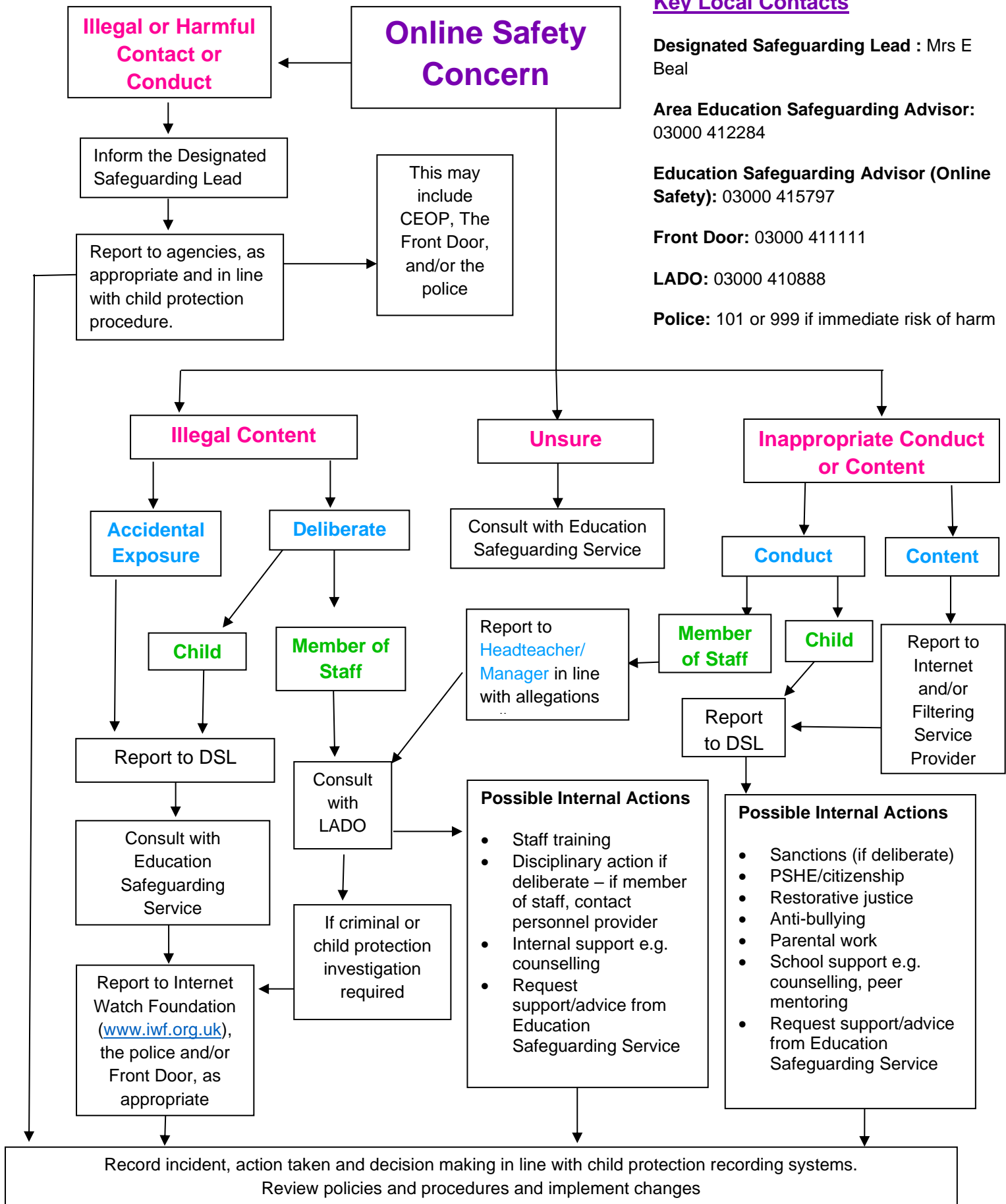
Area Education Safeguarding Advisor: 03000 412284

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm



Useful Links

Kent Educational School Support and Guidance

Education Safeguarding Service, The Education People:

- 03000 415797
 - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
 - Ashley Assiter, Online Safety Development Officer
- Guidance for Educational Schools:
 - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
 - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP: www.kscb.org.uk

Kent Police:

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

Front Door:

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

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

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eisit.uk

National Links and Resources for Schools, 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