

Thurnham C E Infant School



Online Safety Policy Statement

2023-24

Member of Staff Responsible	Mr T Pring/ Mrs E Pateman / Miss S Chastney / Mrs R Evans
Position	Interim Headteacher / Deputy Head & Inclusion Manager/ EYFS / SENCO / Safeguarding Leads
Dated	September 2023 (small, interim revisions as necessary)
Date of next review	September 2024 (or earlier, if large revisions required)

Named Safeguarding Governors: Mrs Lirette Mill & Mr Ben Beer

Key Contacts

	Name	Email
Designated Safeguarding Lead (DSL)	Tony Pring	dsl@thurnham-infant.kent.sch.uk tpring@thurnham-infant.kent.sch.uk
Deputy Designated Safeguarding Lead(s)	Elizabeth Pateman Rebecca Evans Suzanna Chastney	epateman@thurnham-infant.kent.sch.uk revans@thurnham-infant.kent.sch.uk schastney@thurnham-infant.kent.sch.uk
Interim Headteacher	Tony Pring	tpring@thurnham-infant.kent.sch.uk
Safeguarding Governor Contact	Lirette Mill	lmill@thurnham-infant.kent.sch.uk

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

Thurnham C E Infant School Online Safety Policy

This policy is underwritten by our school core Christian value of 'Love' and forms an integral part of all our approaches to everything we do in school.

1. Policy Aims

- This online safety policy has been written involving staff, learners and parents/carers, building on Kent County Councils Education Safeguarding Services policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)', [Early Years and Foundation Stage](#) '[Working Together to Safeguard Children](#)' and our local Safeguarding Children Multi-agency Partnership procedures.
- We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all **pupils** and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate our **pupils** and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.
- Thurnham C of E Infant School understands that breadth of issues classified within online safety is considerable, but can be 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, for example, 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.
- Thurnham C of E Infant School recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online.
- This policy applies to pupils, parents/carers and 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).
- Thurnham C of E Infant School identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all

access to and use of technology, both on and off-site.

- Staff at Thurnham C of E Infant School recognise that some children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected online, and/or they may not recognise their experiences as being abusive or harmful. This should not prevent staff from having professional curiosity and speaking to a DSL if they have any online safety concerns about a child.
- This policy links with several other policies, practices and action plans, including but not limited to:
 - Anti-bullying policy
 - Acceptable Use Policy (AUP)
 - Code of conduct/staff behaviour policy
 - Behaviour policy
 - Child protection policy
 - Confidentiality policy
 - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
 - Data protection
 - Cameras and image use policy
 - Mobile and smart technology
- This policy has also been developed in accordance with the principles established by the Children Acts 1989 and 2004 and related guidance. This includes but is not limited to:
 - Keeping Children Safe in Education 2022 (KCSIE)
 - Working Together to Safeguard Children 2018 (WTSC)
 - Ofsted: Education Inspection Framework' 2022
 - Framework for the Assessment of Children in Need and their Families 2000
 - Kent and Medway Safeguarding Children Procedures
 - Early Years and Foundation Stage Framework 2021 (EYFS)
 - The Education Act 2002
 - Education and Inspections Act 2006
 - The Education (Independent School Standards) Regulations 2014
 - The Non-Maintained Special Schools (England) Regulations 2015

2. Responding to Emerging Risks

- Thurnham CE Infant School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
 - carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our pupils face.
 - 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 is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet 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, and as such identify clear procedures to follow if breaches or concerns arise.

3. Policy monitoring and Review

- Technology evolves and changes rapidly. Thurnham CE Infant School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

4. Roles and Responsibilities

- The governing body have a strategic leadership responsibility for our school's online safeguarding arrangements; they will ensure that they comply with their duties under legislation and will ensure the policies, procedures and training in our school is effective and comply with the law at all times. Tony Pring, Interim Headteacher will ensure that the online safety policies and procedures, adopted by our governing bodies and proprietors, are understood, and followed by all staff.
- The Designated Safeguarding Lead (DSL), Tony Pring, has overall responsibility for the day-to-day oversight of safeguarding and child protection systems, including online safety and understanding the filtering and monitoring systems and processes in place. Whilst the activities of the DSL may be delegated to the deputies, the ultimate lead responsibility for online safety remains with the DSL and this responsibility will not be delegated.

- Whilst the DSL is recognised as holding overall lead responsibility for online safety, however Thurnham CE Infant School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 Leadership and Management

The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of Thurnham CE Infant 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 the DSL and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place but hold overall responsibility for procuring our filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of our provision and overseeing any reports.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of our safeguarding responsibilities, and that a coordinated whole school approach is implemented.
- Taking lead responsibility for overseeing and acting on any concerns identified by our filtering and monitoring systems.

- 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 settings 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, to the Lead DSL and, as appropriate, the Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

4.3 Members of staff

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 Policy.
- 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.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 IT Staff / IT Service Providers

- It is the responsibility of IT staff who are managing our technical environment to:
 - Provide technical support and perspective to the DSL and leadership team in the development and implementation of our online safety policies and procedures, including appropriate filtering and monitoring systems.
 - Support the leadership team and DSL to procure systems, identify risk, carry out reviews and carry out checks to our filtering and monitoring systems:
 - Whilst responsibility for the procurement and implementation of appropriate filtering and monitoring is held by the leadership team and responsibility for acting on safeguarding concerns is led by the DSL; technical staff will ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL to enable them to take appropriate safeguarding action when required.
 - Implement appropriate security measures as directed by the leadership team to ensure that the schools IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

4.5 Pupils

It is the responsibility of pupils (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 school's Acceptable Use Policy.
- 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.

4.6 Parents and carers

It is the responsibility of parents and carers to:

- Read the school AUP and encourage their children to adhere to them.
- Support the school in its online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUP. 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 school online safety policies.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- Thurnham CE Infant School will establish and embed a whole-school culture and will empower our pupils to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- We and will raise awareness and promote safe and responsible internet use amongst pupils/students by:
 - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework](#)' and DfE '[Teaching online safety in school](#)' guidance.
 - ensuring education regarding safe and responsible use precedes internet access.
 - including online safety in the PSHE, Relationship Education and Computing programmes of study, covering use both at home school and home.
 - reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
 - implementing appropriate peer education approaches.
 - educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
 - involving the DSL as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content.
 - making informed decisions to ensure that any educational resources used are appropriate for our pupils.
 - using external visitors, where appropriate, to complement and support our internal online safety education approaches. 'Using External Visitors to Support Online Safety Education: Guidance for Educational Schools' guidance.

- providing online safety education as part of the transition programme across key stages and when moving between establishments.
- rewarding positive use of technology.
- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Thurnham CE Infant School will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
 - ensuring age and/or ability appropriate education regarding safe and responsible use precedes internet access.
 - enabling them to understand what acceptable and unacceptable online behaviour looks like.
 - teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
 - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
 - 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 pupils and those who are potentially at greater risk of harm

- Thurnham CE Infant School recognises that any pupils can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some pupils, for example, looked after children, child who are care leavers, children who are adopted, children who are, or who are perceived to be, lesbian, gay, bi, or trans (LGBT), and those with special educational needs or disabilities (SEND), who may be more susceptible or may have less support in staying safe online.
- Thurnham CE Infant School will ensure that differentiated and appropriate online safety education, access and support is provided to all pupils who require additional or targeted education and/or support.
- Staff at Thurnham CE Infant School will seek input from specialist staff as appropriate, including the DSL or 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, including our acceptable use policy, with all members of staff, including governors as part of induction.
 - provide up-to-date and appropriate training for all staff, including governors, which is integrated, aligned and considered as part of our overarching safeguarding approach.
 - ensure our training for governors equips them with the knowledge to provide strategic challenge to test and assure themselves that our online safety policies and procedures in place in are effective and support the delivery of a robust whole school approach.
 - ensure that online safety training provided to all staff is regularly updated, at least annually.
 - ensure our training covers the potential risks posed to pupils (content, contact and conduct) as well as our professional practice expectations.
 - build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
 - ensure staff are 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.
 - ensure staff are aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
 - highlight useful educational resources and tools which staff could use with pupils.
 - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Thurnham C E Infant School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
 - filtering and monitoring their child's online, providing information in our home-school agreement/AUP.
 - sharing what their children are being asked to do online, including the sites they will asked to access and be clear who from the school (if anyone) their child is going to be interacting with online.

- We will build a partnership approach and reinforce the important of online safety through regular contact and communication with parents and carers by:
 - providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes, and sports days.
 - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our prospectus 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 of technology policies and discuss the implications with their children.

6 Safer Use of Technology

Classroom use

- Thurnham CE Infant school uses a wide range of technology. This includes access to:
 - Computers, laptops, tablets and other digital devices
 - Internet, which may include search engines and educational websites
 - Learning platforms, remote learning platform / tools and intranet
 - Email
 - Games consoles and other games-based technologies
 - Digital cameras, webcams and video cameras.
- All school owned devices will be used in accordance with our acceptable use of technology policy and with appropriate safety and security measures in place.
 - The specific measures in place for tablets are monitored in the same way as other mobile devices, using Smoothwall.
- 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 following an informed risk assessment.
- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place.
- We will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to pupils' age and ability.

Early Years Foundation Stage and Key Stage 1

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

Thurnham C E Infant School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
 - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
 - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's acceptable use policy and is highlighted through a variety of education and training approaches.

6.1 Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an acceptable use policy before being given access to the school computer system, IT resources or internet.

6.2 Decision Making

- Thurnham C E Infant School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's 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 pupils; effective classroom management and regular education about safe and responsible use is essential.

6.3 Filtering

- The school purchases broadband connectivity through EIS / Cantium Schools Broadband.
- The school uses the Smoothwall web filtering system which blocks sites which can be categorised as of a 'sensitive' nature: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
 - The school filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- The school works with EIS Schools Broadband to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

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

6.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
 - *EIS Schools Broadband sends a report to the Headteacher and Safeguarding Lead which demonstrates any use or access to websites of concern. Action is taken as necessary on the content of the report.*
- The school has a clear procedure for responding to concerns identified via monitoring approaches as the DSL will respond in line with the child protection policy.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

6.5 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.

6.6 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly.
 - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
 - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on the school's network.
 - The appropriate use of user logins and passwords to access the school network.
 - All users are expected to log off or lock their screens/devices if systems are unattended.

6.7 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.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords every forty days.
 - 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.

6.8 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

6.9 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): Image use policy, Data security, Codes of conduct, Social media and use of personal devices and mobile phones.

6.10 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: confidentiality, acceptable use policy and 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 for setting up personal social media accounts.
- Members of the school community will immediately tell the DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

6.11 Staff

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

6.12 Pupils

- Pupils may use school provided email accounts for educational purposes.
- Pupils will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the school.

6.13 Educational use of Videoconferencing and/or Webcams

- Thurnham C E Infant School recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
 - All videoconferencing 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.
- Videoconferencing contact details will not be posted publicly.
- School videoconferencing equipment will not be taken off school 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.

6.14 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
- Videoconferencing 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 remotely-controlled 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.

6.15 Content

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

6.16 Management of Learning Platforms / Live Inputs

- Thurnham C E Infant School uses Kent Learning Zone / SharePoint (for staff) and Seesaw as its official learning platform for home learning.
- When appropriate, any home learning requiring live input or teaching is through a Microsoft Teams link. Teachers carefully check that all children's home cameras and microphones are switched off

when asked to do so or as appropriate, control this centrally. This is particularly important and is checked should a session have to be recorded. Parents are asked to stay in close supervision if sessions are taking place with the children fully dressed for the day.

- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the LP.
- When staff and/or pupils leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils and staff 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 pupil's parent/carer may be informed.
 - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil 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.

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

- The school uses the SIMS system to track pupils progress and share appropriate information with parents and carers.
- The headteacher 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
- In order to safeguard pupils' data:
 - Only school issued devices will be used for apps that record and store children's 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 children's personal details, attainment or images.
 - School 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.

7. Social Media

7.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Thurnham C E Infant School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Thurnham C E Infant School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
 - All members of Thurnham C E Infant School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
 - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Thurnham C E Infant School community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Disciplinary, Behaviour and Safeguarding policies as well as the staff Code of Conduct document.

7.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of Conduct within the AUP.

Reputation

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

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - Setting the privacy levels of their personal sites as strictly as they can.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Thurnham C E Infant School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also 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 with the school's 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 pupils 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 in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
 - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or Headteacher.
 - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

7.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies (including anti-bullying and behaviour). Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
 - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications and report concerns both within school and externally.

7.4 Official Use of Social Media

Thurnham C E Infant School does not use or run its own social media.

8 Use of Personal Devices and Mobile Phones

- Thurnham C E Infant School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

8.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.

- All members of Thurnham C E Infant School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of Thurnham C E Infant 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 the potential presence of children i.e. classrooms, the school hall, etc.
- The sending of abusive or inappropriate messages / content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of Thurnham C E Infant School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or child protection policies.

8.2 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 school policy and procedures, such as: Confidentiality, Safeguarding, Data Security and Acceptable Use Policy.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time (e.g. locked in a locker/drawer)
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances.
 - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Leads.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
 - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
 - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.

- If a member of staff breaches the school policy, action will be taken in line with the school disciplinary 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.

8.3 Pupils' Use of Personal Devices and Mobile Phones

- Although as an infant school, we do not allow the children to carry mobile phones, pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

8.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's acceptable use policy and other associated policies, such as: Mobile Phone Policy, Anti-bullying, Behaviour, Child Protection and Image Use Policy.
- The school will ensure appropriate signage and information is displayed / 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 Designated Safeguarding Lead of any breaches of school policy.

9 Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
 - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.

- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10 Concerns about Pupils Welfare

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

10.1 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Safeguarding and Disciplinary policies.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Safeguarding and Disciplinary policies and Code of Conduct.

11 Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online sexual violence and sexual harassment between children

- Our 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 '[Keeping children safe in education](#)' 2022.
 - Full details of our response to peer-on-peer abuse, including sexual violence and harassment can be found in our child protection policy.
- Thurnham CE Infant School recognises that sexual violence and sexual harassment between children can take place online. Examples may include;
 - Non-consensual sharing of sexual images and videos.
 - Sexualised online bullying.
 - Online coercion and threats.
 - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence.

- Unwanted sexual comments and messages on social media.
- Online sexual exploitation.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
 - immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
 - if content is contained on learners' personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
 - implement appropriate sanctions in accordance with our behaviour policy.
 - inform parents and carers, if appropriate, about the incident and how it is being managed.
 - If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
 - if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
 - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
 - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Thurnham CE Infant 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.
- Thurnham CE Infant School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns Thurnham CE Infant 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 or "Sexting"

- Thurnham C E Infant School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue should our infant pupils come into contact with it (e.g. via an older sibling); therefore, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

- The school will follow the advice as set out in the non-statutory UKCCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) and KSCB guidance: “Responding to youth produced sexual imagery”.
- Thurnham C E Infant 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.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.3 Dealing with ‘Sexting’

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
 - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board’s procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store the device securely.
 - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Specialist Children’s Services and/or the Police, as appropriate.
 - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
 - Implement appropriate sanctions in accordance with the school’s Behaviour policy but taking care not to further traumatise victims where possible.
 - Consider the deletion of images in accordance with the UKCCIS: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
 - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.

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

11.4 Online Child Sexual Abuse and Exploitation

- Thurnham C E Infant 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.
- Thurnham C E Infant School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community (e.g. school website, class computers etc.).

11.5 Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's Child Protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Make a referral to Specialist Children's Services (if required / appropriate).
 - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
 - Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](#) (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.6 Indecent Images of Children (IIOC)

- Thurnham C E Infant School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
 - Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.

- Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
 - Ensure that the headteacher is informed.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Quarantine any devices until police advice has been sought.

11.7 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Thurnham C E Infant School.
- Full details of how the school will respond to cyberbullying are set out in our Anti-bullying policy.

11.8 Online Hate

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

11.9 Online Radicalisation and Extremism

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

- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with our Safeguarding and Allegations policies.

Kent Educational Setting Support and Guidance

Education Safeguarding Service, 'The Education People' contacts are shown at the end of this document:

- Key Online Safety Number: 03301651500
- Guidance for Educational Settings:
 - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
 - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP: www.kscb.org.uk

Kent Police:

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

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

Other:

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

National Links and Resources for Settings, Learners and Parents/carers

CEOP:

- www.thinkuknow.co.uk
- www.ceop.police.uk

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

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

UK Safer Internet Centre: www.saferinternet.org.uk

- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Report Harmful Content: <https://reportharmfulcontent.com/>

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

Childnet: www.childnet.com

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

Internet Matters: www.internetmatters.org

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

Parent Info: <https://parentinfo.org>

NSPCC: www.nspcc.org.uk/online-safety

- 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

Education Safeguarding Service Contacts

Head Office: Room 2.30 Sessions House, County Hall, Maidstone ME14 1XQ	
Claire Ray Head of Service	03301 651 200
Rebecca Avery Training & Development Manager	03301 651 110
Robin Brivio Senior Safeguarding Advisor	03301 651 200
Online Safety	03301 651 500
For advice on safeguarding issues please call your area office on the numbers listed below. If a child may be at risk of imminent harm, you should call the Integrated Front Door on 03000 411 111 or the Police on 999	
Ashford	03301 651 340
Canterbury	03301 651 140
Dartford	03301 651 240
Dover	03301 651 340
Folkestone & Hythe	03301 651 340
Gravesham	03301 651 240
Maidstone	03301 651 440
Sevenoaks	03301 651 240
Swale	03301 651 140
Thanet	03301 651 140
Tonbridge & Malling	03301 651 440
Tunbridge Wells	03301 651 440

Kent County Council Key Contacts

Integrated Front Door: 03000 411 111 (outside office hours **03000 419 191**)

Early Help Contacts (district teams) can be found on www.kelsi.org.uk

LADO Team contact number: 03000 410 888

If your call is urgent i.e. a child is in **immediate danger** and you cannot be connected to the team, call the Integrated Front Door on **03000 411 111**

Email: kentchildrenslado@kent.gov.uk

Kroner House, Eurogate Business Park, Ashford, Kent, TN24 8XU

Area Education Officers

South Kent – Lee Round 03000 412 309

East Kent – Marisa White 03000 418 794

West Kent – Nick Abrahams 03000 410 058

North Kent – Ian Watts 03000 414 302

Prevent Education Officers

North/West/ Medway - Sally Green sally.green2@kent.gov.uk 03000 413 439

South/East - Jill Allen jill.allen@kent.gov.uk 03000 413 565