

Viking Academy Trust



Online Safety Policy

Approved by the Trust: Term 1 2018

Reviewed every year. Also revised following any changes to technology use, online safety concerns and/or updates to national and local guidance or procedures.

Last review date: Term 2 2025

Signed



Chair of Trust

Online Safety Policy

The Viking Academy Trust

Empowering Children Through Education: One Childhood One Chance

Schools in the Viking Academy Trust (VAT)

Chilton Primary School
Ramsgate Arts Primary School
Upton Junior School

This Online Safety Policy is specific to Chilton Primary School

Key Details

Designated Safeguarding Leads: Alex McAuley, Hannah Cheshire
Named governor with lead responsibility: Natalie Barrow
Trustee with lead responsibility: Joanna Brand
Trust Leaders with responsibility: Kate Law / Lisa Blatchford

1. Policy Aims and Scope

- This policy has been written by Chilton Primary School, involving staff, pupils and parents/carers, building on the Kent County Council LADO Education Safeguarding Advisory Service 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.
 - [Home - Kent Safeguarding Children Multi-Agency Partnership](#)
 - [Home - KELSI](#)
- 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.
- Chilton Primary 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, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
 - **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.
- Chilton Primary 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).
 - Chilton Primary School recognises that the internet and technology, including computers, tablets, mobile devices, wearable technology, game consoles, email and social media, is central to daily life, offering both opportunities and risks. This policy covers all technology use, whether on or off-site.
 - Staff Chilton Primary School recognise that 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 Policies (AUP)
 - Code of conduct
 - 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
 - Image use policy
 - Mobile and smart technology and Social Media

1. Responding to Emerging Risks

- Chilton Primary 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.

2. Policy monitoring and review

- Technology evolves and changes rapidly. Chilton Primary 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 Head of School 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.
- All members of the community will be made aware of how our school will monitor policy compliance: Through AUPs, staff training and classroom management.

3. 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. Alex McAuley (Head of School) 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 Leads (DSLs – Alex McAuley and Hannah Chesire) have 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, Chilton Primary 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 school culture that incorporates online safety throughout.
 - 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 which address the acceptable use of technology, child-on-child abuse, use of social media and mobile technology.
 - Work with the DSL and IT Staff 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 regarding online safety concerns.
 - Undertake appropriate risk assessments regarding the safe use of technology on site.
 - Audit and evaluate online safety practice to identify strengths and areas for improvement. Ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety.
 - Support staff to ensure that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL):

- The leadership and management team will:
 - Act as a named point of contact on all online safeguarding issues.
 - Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO) on matters of online safety as appropriate.
 - 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 and up-to-date knowledge required to keep **pupils** safe online, including the additional risks that **pupils** with Special Educational Needs 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 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 (at least 3 times per year) with the governor with a lead responsibility for safeguarding (this includes online safety)

4.3 Members of staff

- It is the responsibility of all members of staff to:
 - Contribute to the development of our online safety policies.
 - Read and adhere to our online safety policy and acceptable use of technology policies.
 - Take responsibility for the security of devices, systems and the electronic data they use or have access to.
 - Model good practice when using technology with pupils.
 - Maintain a professional level of conduct in their personal use of technology, both on and off site.
 - Embed online safety education in curriculum delivery wherever possible.
 - Have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care.
 - Identify online safety concerns and take appropriate action by following our safeguarding policies and procedures.
 - Know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally.
 - Take personal responsibility for professional development in this area.

4.4 IT Staff

- 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 including (phishing simulations, filtering and monitoring checks) 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

- Pupils have a right to:
 - Feel safe online and have their views and feelings considered.
 - Confidently report online abuse or exploitation, knowing their concerns will be taken seriously.
 - Contribute to the development of school online safety policies.
 - Receive help from a trusted adult.
 - Learn how to keep themselves safe online.
- It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:
 - Engage in age/ability appropriate online safety education.
 - 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.

4.6 Parents/carers

- It is the responsibility of parents and carers to:
 - Read our Acceptable Use of technology policies and encourage their child(ren) to adhere to them.
 - Support our online safety approaches by discussing online safety issues with their child(ren) 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 and acceptable use of technology policies.
 - Seek help and support from the school or other appropriate agencies if they or their child(ren) encounter online issues.
 - Contribute to the development of our online safety policies.
 - Use our systems, such as learning platforms and other IT resources, safely and appropriately.
 - Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their child(ren) access and use at home.

5.

Education and Engagement Approaches

5.1 Education and engagement with pupils

- Chilton Primary 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 by:

- ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework](#)' and DfE '[Teaching online safety in school](#)' guidance.
 - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study (using school's own curriculum materials informed by The PSHE Association and other resources)
 - reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
 - implementing appropriate peer education approaches (e.g. monitors, the IT Gang, Thrive Ambassadors)
 - 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.
 - providing online safety education as part of the transition programme across the key stages and when moving between establishments.
 - rewarding positive use of technology through curriculum incentives and behaviour policies.
- Chilton Primary School will support pupils to understand and follow our Acceptable Use policies in a way which suits their age and ability by:
 - sharing our acceptable use policies with them in accessible and appropriate ways.
 - 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 pupils voice when writing and developing online safety policies and practices, including curriculum development and implementation.
 - Chilton Primary 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

- Chilton Primary 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, bisexual, trans (LGBT) or gender questioning, and those with special educational needs or disabilities (SEND), who may be more susceptible or may have less support in staying safe online.
- Chilton Primary 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. This will be achieved through adjusted planning, resources and support.
- Staff at Chilton Primary School will seek input from specialist staff as appropriate, including the DSL, SENCO, Designated Teacher 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 and trustees as part of induction.
 - provide up-to-date and appropriate training for all staff, including governors and trustees, which is integrated, aligned and considered as part of our overarching safeguarding approach. This is provided at least annually with regular updates as required and at induction during the school year.
 - ensure our training for governors and trustees 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 and through updates as appropriate throughout the school year)
 - 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

- Chilton Primary School recognises that parents and carers have an essential role to play in enabling our pupils to become safe and responsible users of the internet and associated technologies.
- We will ensure parents and carers understand and are aware of:
 - the systems used at school to filter and monitor their child's online use by sharing of our AUPs
 - what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online by sharing termly and weekly curriculum information
- 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 (through information sent home, curriculum events and information).
 - 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 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

6.1 Classroom use

- Chilton Primary School uses a wide range of technology. This includes access to:
 - Computers, laptops and tablets
 - Internet, which may include search engines and educational websites
 - Learning platforms, remote learning platform/tools and intranet
 - Digital cameras, webcams and video cameras.
- All school owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place including the sign-in requirement for all devices
- 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.
- 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. Video platforms are only available on staff devices

- 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. This includes
 - **Early Years Foundation Stage and Key Stage 1**
 - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils age and ability.
 - **Key Stage 2**
 - Pupils will use age-appropriate search engines and online tools.
 - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils age and ability.

6.2 Generative Artificial Intelligence (AI)

- Chilton Primary School recognises that when used safely, effectively and with the right infrastructure in place, generative artificial intelligence (AI) tools have many uses which could benefit our entire community.
- However, it is important to recognise that AI tools can also pose safeguarding risks to our community as well as moral, ethical and legal concerns. This includes, but is not limited to:
 - exposure to inappropriate or harmful content, including bullying, harassment, abuse and exploitation
 - privacy and data protection breaches/risks
 - intellectual property infringements
 - academic integrity challenges such as plagiarism and cheating
 - exposure to inaccurate, misleading, or biased content.
- Chilton Primary School only permits the use of generative AI tools which have been approved and provided by the school for work and/or educational purposes, following the senior leadership team undertaking risk assessments and data protection impact assessments (as appropriate) prior to use.
- Staff and pupils will be made aware of the benefits and risks of using generative AI tools and the school expectations by staff training, AUP and AI policy
- Chilton Primary School will respond to any misuse of AI in line with relevant policies, including but not limited to, anti-bullying, behaviour, data protection, complaints and child protection.
- Where the school believe that AI tools may have facilitated the creation of child sexual abuse material, the school will respond in line with existing local safeguarding procedures and [national guidance](#) from the IWF and NCA-CEOP.
- Where the school are responding to concerns regarding digitally manipulated and AI-generated nudes and semi-nudes, the school will respond in line our child protection policy, with section 11.1.2 of this policy and the local [KSCMP](#) safeguarding procedures and UKCIS '[Sharing nudes and semi-nudes: advice for education settings working with children and young people](#)' guidance.
- Where the school believe that AI tools may have facilitated [deep fake](#) abuse of adults, advice and support will be provided to individuals affected, such as via Unions, [Professionals Online Safety Helpline](#) or [Report Harmful Content](#) and/or if a crime has been committed, via the [police](#).

Action will be taken in line with relevant school policies, including but not limited to, anti-bullying, behaviour and complaints.

6.3 Managing internet access

- All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role, before being given access to our computer system, IT resources or the internet.
- We will maintain a record of users who are granted access to our devices and systems.

6.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with UK General Data Protection Regulations (UK GDPR) and Data Protection legislation.
 - Full information can be found in our information security policy which can be accessed at www.vikingacademytrust.com

6.5 Information security and access management

- We take appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and pupils.
- Further information about technical environment safety and security can be found in separate technical policies or procedures that contain other relevant information, but includes:
 - Virus protection being updated regularly.
 - Encryption for personal data sent over the Internet or taken off site or access via appropriate secure remote access systems.
 - 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 and user logins and passwords will be enforced for all users in KS2 and staff
 - All users are expected to log off or lock their screens/devices if systems are unattended.
- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.

6.4.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 3, all pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.

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

6.6 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 school 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 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.

6.7 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 cameras and image use, data security, acceptable use policies, codes of conduct social media and use of personal devices and mobile phones policies.

6.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and 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 report offensive communication to Alex McAuley and Hannah Cheshire (Designated Safeguarding Leads)
- Excessive social email use can interfere with teaching and learning and will not be permitted at all during this time.

6.8.1 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.
 - are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.

6.9 Educational use of videoconferencing and/or webcams

- Chilton Primary School recognises that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
 - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
 - Videoconferencing 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.
 - Videoconferencing equipment will not be taken off the premises
 - Staff will ensure that external videoconferencing opportunities and tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
 - Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

6.8.1 Users

- Parents/carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will take place via official and approved communication channels following a robust risk assessment and will be supervised appropriately, according to the pupils age and ability.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and will be kept securely, to prevent unauthorised access.

6.8.2 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, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the pupils.

6.9 Management of remote learning

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

- Chilton Primary School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with pupils and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and agreed systems (Microsoft Teams)
 - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and pupils will engage with remote teaching and learning in line with existing behaviour principles as set out in our code of conduct and Acceptable Use Policies.
- Staff and pupils will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP)
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Chilton Primary School will continue to be clear who from the school their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

7. Appropriate Filtering and Monitoring on School Devices and Networks

- Chilton Primary School will do all we reasonably can to limit children’s exposure to online harms through school provided devices, systems, platforms and networks. In line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.
- This includes ensuring application of appropriate filtering and monitoring to both static content, as well as dynamic and AI-generated materials, products and/or systems used.
- When implementing appropriate filtering and monitoring, Chilton Primary School will ensure that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach, and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils. Effective safeguarding practice, robust policies, appropriate classroom/ behaviour management and regular education/ training about safe and responsible use is essential and expected.
- Pupils will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment. For example, using a child friendly search engine, using child friendly tools.

- Internet use will be supervised by staff as appropriate to pupils age, ability and potential risk of harm

7.1 Responsibilities for filtering and monitoring

- Our governing body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate safeguarding concerns when identified.
- Alex McAuley, a member of the senior leadership team and Natalie Barrow, governor, are responsible for ensuring that our school has met the DfE [Filtering and monitoring standards](#) for schools and colleges.
- Our senior leadership team is responsible for:
 - procuring our filtering and monitoring systems.
 - documenting decisions on what is blocked or allowed and why.
 - reviewing the effectiveness of our provision.
 - overseeing reports.
 - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
 - ensuring the DSL and IT staff have sufficient time and support to manage their filtering and monitoring responsibilities.
- The DSL has lead responsibility for overseeing and acting on:
 - any filtering and monitoring reports.
 - any child protection or safeguarding concerns identified.
 - checks to filtering and monitoring system.
- The IT staff have technical responsibility for:
 - maintaining filtering and monitoring systems.
 - providing filtering and monitoring reports.
 - completing technical actions identified following any concerns or checks to systems.
 - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.
- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.
- All staff, pupils and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

7.2 Decision making and reviewing our filtering and monitoring provision

- When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team works closely with the DSL and the IT staff.
- Decisions about our filtering and monitoring provision have been recorded and informed by an approach which ensures our systems meet our school needs and circumstances, including but

not limited to our pupil risk profile which considers the specific vulnerabilities (including age and ability), risk and context of our pupils and our school specific technology use.

- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and with approval from the leadership team; all changes to the filtering policy are logged and recorded.
- Our school undertakes regular (at least annual) reviews of our filtering and monitoring approaches to ensure we understand the changing needs and potential risks posed to our community.
- In addition, our school undertakes regular and active checks on our filtering and monitoring systems to ensure our systems work effectively in practice and as expected, and to provide assurance to the governing body that we are continuing to meet our safeguarding obligations. These checks are logged and recorded.
- These checks are achieved by:
 - Daily blocked reports sent to Heads
 - Filtering and Monitoring checks 3 times per year (reported to Governing body) – testing search terms that check appropriate filtering and monitoring and also using TestFiltering. This is completed on staff and pupil devices.
 - Records of these are kept electronically and also shared and governors meetings

7.3 Appropriate filtering

- Chilton Primary School 's education internet connectivity is provided through LGfL and [Chilton Primary School uses netsweeper to block access to harmful content.
- Netsweeper blocks school provided internet access to illegal content and activity as identified in the Online Safety Act, including:
 - Child Sexual Abuse Material (CSAM)
 - Controlling or coercive behaviour
 - Extreme sexual violence
 - Extreme pornography
 - Fraud
 - Racially or religiously aggravated public order offences
 - Inciting violence
 - Illegal immigration and people smuggling
 - Promoting or facilitating suicide
 - Intimate image abuse
 - Selling illegal drugs or weapons
 - Sexual exploitation
 - Terrorism
- Netsweeper is a member of [Internet Watch Foundation](#) (IWF) and uses IWF services to block access to CSAM.
- Netsweeper has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Netsweeper blocks school provided internet access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content or activity which promotes hate speech or discrimination, gambling, harmful bullying content, malware/hacking, mis-disinformation, privacy and copyright theft, pornography, self-harm and eating disorders and/or violence against women and girls

- Our filtering system is operational, up to date and applied to all users, including guest accounts, all school owned or provided devices, systems and networks, and all devices using the school internet connection.
- The DSL and leadership team will work with LGfL and our IT service staff as appropriate and as identified in section 6.3.2, to ensure that our filtering policy is continually checked and reviewed to reflect our needs and requirements.
- If there is failure in the software or abuse of the system, for example if pupils or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:
 - Close the lid of a laptop or press the home button on an ipad (pupils)
 - Report the issue to a member of staff
 - Staff will report the issue to a DSL and member of IT staff
- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and Code of Conduct
- Parents/carers will be informed of filtering breaches involving their child, unless to do so would put a child at risk of harm or compromise a criminal investigation.
- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the [Internet Watch Foundation](#) (where there are concerns about child sexual abuse material), the police (either via 101 or 999 if an emergency or [NCA-CEOP](#)) or Children's Social Care.
- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

7.4 Appropriate monitoring

- We will appropriately monitor the use of all school provided devices and networks to detect safeguarding risks in real or near-real time, including accessing or attempting to access, or engaging with or attempting to engage with illegal and/or harmful/inappropriate content or activity by any user. This is achieved by:
 - Daily logs being sent to DSLs
 - Supervision of internet access
- In accordance with our Mobile and Smart Technology Policy, Chilton Primary School does not allow use of personal devices by staff and pupils.
- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
 - Where the concern relates to pupils it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies.
 - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the Head of School), in line with our staff Code of Conduct and Allegations policy
 - Parents/carers will be informed of safeguarding concerns involving their child identified through our monitoring approaches, unless to do so would put a child at risk of harm or compromise a criminal investigation.

- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, the Police via 101 or [NCA-CEOP](#) , the LADO or Children’s Social Care.

8.1 Expectations

- Chilton Primary School believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.
 - The applies to all use of social media including, but not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.
- All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will restrict learner and staff access to social media via our filtering and monitoring systems which are applied to all school provided devices and systems. Social media sites are blocked (apart from Youtube on staff devices).
- Concerns regarding the online conduct of any member of Chilton Primary School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff code of conduct, Acceptable Use Policies, and child protection.

8.2 Staff use of social media

- The use of social media during school hours for personal use is only permitted in break times in staff only spaces (i.e. the staff room)
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

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. This may include, but is not limited to:
 - Setting appropriate privacy levels on their personal accounts/sites.
 - Being aware of the implications of using location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Using strong passwords.
 - Ensuring staff do not represent their personal views as being that of the school.

- Members of staff are encouraged not to identify themselves as employees of Chilton Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All 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 reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- 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.

8.2.2 Communicating with pupils and their families

- Staff will not use any personal social media accounts to contact pupils or their family members.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media accounts.
- Any communication from pupils and parents/carers received on personal social media accounts will be reported to the DSL (or deputy)
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL
- Decisions made and advice provided in these situations will be formally recorded to safeguard pupils members of staff and the setting.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

8.3 Official use of social media

- Chilton Primary School official social media channels are:
 - [\(1\) Facebook](#)
 - [ChiltonRamsgate \(@chiltonramsgate\)](#) • [Instagram photos and videos](#)
 - [Twitter – Chilton Ramsgate](#)
- The official use of social media sites by Chilton Primary School only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the Head of School prior to use.
- Official social media sites are suitably protected
 - Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
 - Staff use setting provided email addresses to register for and manage official social media channels.
 - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.

- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with pupils; any official social media activity involving pupils will be moderated if possible and written parental consent will be obtained as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- 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 managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
 - Read and understand our 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.
 - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
 - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - Not engage with any private or direct messaging with current or past pupils or their family members.
 - Inform their line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

8.4 Pupils use of social media

- The use of social media during school hours for personal use is not permitted for pupils.
- Many online behaviour incidents amongst children occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, where online behaviour poses a threat or causes harm to another pupils could have repercussions for the orderly running of the school when the pupils is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection and online safety policies.
- Chilton Primary School will empower our pupils to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies (e.g. RSE)
- Pupils will be advised:
 - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.

- to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
 - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
 - to use safe passwords.
 - to use social media sites which are appropriate for their age and abilities.
 - how to block and report unwanted communications.
 - how to report concerns on social media, both within the setting and externally.
- Any concerns regarding pupils use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
 - The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
 - Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
 - Concerns regarding pupils use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
 - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL **and/or** headteacher.
 - documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
 - Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy.

9. Responding to Online Risks and/or Policy Breaches

- 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.
 - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This may include:
 - Low Level Concern
 - AUP
 - Use of social media and technology
 - Child Protection
 - Allegations
 - will respect confidentiality and the need to follow the official procedures for reporting concerns.
 - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
 - will be made aware of how the school will monitor policy compliance by:
 - AUPs, staff training, classroom management.
 - are expected to adopt a partnership with the school to resolve issues.

- If appropriate, after any investigations are completed, the DSL and 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 headteacher will seek advice from the local authority or other agency in accordance with our child protection policy (through online contact to LESAS)
- 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.
- 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 or Head of School will speak with the police and/or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about pupil online behaviour and/or welfare

- Chilton Primary School recognises that an initial disclosure to a trusted adult may only be the first incident reported, rather than representative of a singular incident and that trauma can impact memory, so children may not be able to recall all details or timeline of abuse. All staff will be aware certain children may face additional barriers to telling someone, for example because of their vulnerability, disability, sex, ethnicity, and/or sexual orientation.
- All concerns about pupils will be responded to and recorded in line with our child protection policy:
 - The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
 - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Abuse that occurs online and/or offsite will not be dismissed or downplayed; concerns will be treated equally seriously and in line with relevant policies/procedures, for example anti-bullying, behaviour, child protection, online safety.
- Chilton Primary School recognises that the law is in place to protect children rather than criminalise them, and this will be explained in such a way to pupils that avoids alarming or distressing them.
- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to pupils as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required, unless to do so would place a child at risk or harm or would undermine a criminal/safeguarding investigation.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be managed in accordance with our allegations against staff policy/staff code of conduct
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

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 headteacher and/or DSL and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

11. Procedures for responding to specific online concerns

11.1 Online child-on-child abuse

- Chilton Primary School recognises that whilst risks can be posed by unknown individuals or adults online, pupils 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.
- We recognise that online child-on-child abuse can take many forms, including but not limited to:
 - bullying, including cyberbullying, prejudice-based and discriminatory bullying
 - abuse in intimate personal relationships between peers
 - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
 - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
 - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as ‘sexting’ or ‘youth produced sexual imagery’)
 - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
 - upskirting (which is a criminal offence), which typically involves taking a picture under a person’s clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
 - initiation/hazing type violence and rituals.
- Chilton Primary School adopts a zero-tolerance approach to child-on-child abuse. We believe that abuse is abuse and it will never be tolerated or dismissed as “just banter”, “just having a laugh”, “part of growing up” or “boys being boys”; this can lead to a culture of unacceptable behaviours and can create an unsafe environment for children and a culture that normalises abuse, which can prevent children from coming forward to report it.
- Chilton Primary School believes that all staff have a role to play in challenging inappropriate online behaviours between children. Staff recognise that some online child-on-child abuse issues may be affected by gender, age, ability and culture of those involved.
- Chilton Primary School recognises that even if there are no reported cases of online child-on-child abuse, such abuse is still likely to be taking place, and it may be the case that it is just not being reported. As such, it is important that staff speak to the DSL (or deputy) about any concerns regarding online child-on-child abuse.
- Concerns about child-on-child abuse taking place online offsite will be responded to as part of a partnership approach with pupils’ and parents/carers; concerns will be recorded and responded to in line with existing appropriate policies, for example anti-bullying, acceptable use, behaviour and child protection policies. Note: section 89(5) of the Education and Inspections Act 2006 gives headteachers a statutory power to discipline pupils for poor behaviour outside of the

school premises, for example, when children are not under the lawful control or charge of a member of school staff, to such extent as is reasonable.

- Chilton Primary School wants children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child-on-child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Pupils who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

11.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Chilton Primary School will follow the guidance outlined in Part Five of KCSIE.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.
- Chilton Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
 - consensual and non-consensual sharing of nude and semi-nude images and videos
 - sharing of unwanted explicit content
 - ‘upskirting’ (which is a criminal offence and typically involves taking a picture under a person’s clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
 - sexualised online bullying
 - unwanted sexual comments and messages, including, on social media
 - sexual exploitation, coercion and threats.
- Chilton Primary School recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce complex factors. These include the potential for the incident to take place across several social media platforms and services, and for things to move from platform to platform online.
- Chilton Primary School 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.
- Chilton Primary 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 and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator, and any other children involved/impacted.
 - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.

- Reports will initially be managed internally by the DSL, and where necessary will be referred to Children’s Social Care and/or the police.
 - The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
 - If content is contained on pupils personal devices, they will be managed in accordance with the DfE [‘searching screening and confiscation’](#) advice
- Following an immediate risk assessment, the school will:
 - provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
 - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
 - if the concern involves children 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 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.
 - Chilton Primary School recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Chilton Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

11.1.2 Nude or semi-nude image sharing

- Chilton Primary School recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or “sexting”) is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
 - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
 - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
 - possesses nude and/or semi-nude imagery created by another person under the age of 18.
- When made aware of concerns regarding nude and/or semi-nude imagery, Chilton Primary School 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’](#)

- Chilton Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
 - Report any concerns to the DSL immediately.
 - Never view, copy, print, share, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already inadvertently viewed imagery, this will be immediately reported to the DSL.
 - Not delete the imagery or ask the child to delete it.
 - Not say or do anything to blame or shame any children involved.
 - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
 - Not ask the child or children involved in the incident to disclose information regarding the imagery.
 - to not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
 - act in accordance with our child protection policies and the relevant local procedures and in line with the [UKCIS](#) guidance.
 - carry out a risk assessment in line with the [UKCIS](#) guidance which considers the age and vulnerability of pupils involved, including the possibility of carrying out relevant checks with other agencies.
 - a referral will be made to Children’s Social Care and/or the police immediately if:
 - the incident involves an adult (over 18).
 - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
 - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child’s developmental stage, or are violent.
 - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
 - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
 - If DSLs are unsure how to proceed, advice will be sought from the local authority.
 - Store any devices securely:
 - If content is contained on pupils 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.
 - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.

- provide the necessary safeguards and support for pupils such as offering counselling or pastoral support.
 - implement sanctions where necessary and appropriate 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.
 - Pupils will be supported in accessing the Childline '[Report Remove](#)' tool where necessary: Report Remove Tool for nude images.
 - 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.
- We will not:
 - view any 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 in line with the national [UKCIS guidance](#), 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 and will not allow or request pupils to do so.

11.1.3 Cyberbullying

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

11.2 Responding to potentially illegal content and/or activity online

- In accordance with the [Online Safety Act](#), and other relevant legislation including but not limited to the Sexual Offences Act, Criminal Justice and Immigration Act, the Serious Crime Act, Malicious Communication Act, Protection from Harassment Act, Chilton Primary School understands the following content and activity is considered to be illegal:
 - child sexual abuse, including child sexual abuse material (CSAM)
 - controlling or coercive behaviour
 - cyberflashing
 - encouraging or assisting serious self-harm
 - epilepsy trolling
 - extreme sexual violence
 - extreme pornography
 - fraud
 - racially or religiously aggravated public order offences
 - inciting violence
 - intimate image abuse
 - illegal immigration and people smuggling
 - promoting or facilitating suicide
 - intimate image abuse
 - selling illegal drugs or weapons
 - sending false information intended to cause non-trivial harm

- sexual exploitation
 - terrorism
 - threatening communications
- The DSL holds overall responsibility for responding to child protection concerns or incidents involving potentially illegal content or activity.
 - Any suspected exposure to illegal content must be treated as a safeguarding concern and reported to the DSL without delay and managed in line with our child protection and behaviour policies.
 - The DSL will ensure that staff are trained to identify and report such concerns appropriately.

The DSL will assess the concern and determine the appropriate response, which may include:

- Taking immediate safeguarding actions to protect any child(ren) involved.
 - Recording the incident in line with existing school policies and notifying senior leadership.
 - Reporting to external agencies in line with local safeguarding procedures, including Children’s Social Care, and/or the police, as appropriate.
 - Reporting to national organisations, such as the Internet Watch Foundation (IWF) or CEOP as appropriate.
- If concerns relate to a member of staff accessing illegal content or engaging in illegal activity, the school will ensure that the headteacher is informed in line with our managing allegations against staff policy and inform the LADO and other relevant organisations, such as the police, in accordance with our managing allegations against staff policy.

11.2.3 Online child abuse and exploitation

- Chilton Primary 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, in line with our child protection policy.
- Chilton Primary 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 pupils and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- 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 local safeguarding children partnership procedures.
 - store any devices containing evidence securely:
 - If content is contained on pupils 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 via the locally agreed safeguarding arrangements, and inform the police via 101, or 999 if a pupil is at immediate risk.

- carry out a risk assessment which considers any vulnerabilities of pupils involved, including carrying out relevant checks with other agencies.
 - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
 - provide the necessary safeguards and support for pupils such as, offering counselling or pastoral support.
 - review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
 - Where possible and appropriate, pupils will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
 - If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority and/or police.
 - We will ensure that the NCA-CEOP reporting tools are visible and available to pupils and other members of our community.
 - 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.
 - If members of the public or pupils at other schools or settings are believed to have been targeted, the DSL, will seek advice from the police and/or the Local Authority before sharing specific information to ensure that potential investigations are not compromised.
 -

11.2.4 Child Sexual Abuse Material (CSAM)

- Chilton Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Child Sexual Abuse Material (CSAM), also known as [Indecent Images of Children \(IIOC\)](#), as appropriate.
 - These terms also apply to [pseudo-images](#) which are computer-generated images that otherwise appear to be a photograph or video. These may be created using tools such as photo/video editing software, deepfake apps and generators (to combine and superimpose existing images or videos onto other images and videos), and AI text-to-image generators.
 - Any concerns related to consensual and non-consensual nude or semi-nude images sharing by children, will be responded to in line with section 11.1.2 of this policy.
- We will respond to concerns regarding CSAM on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to CSAM 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 will obtain advice immediately through the police and/or the Local Authority.
- If made aware of concerns relating to CSAM, we will:

- act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures.
- lock/limit access and store any devices involved securely to prevent further viewing or deletion of evidence etc, until advice has been sought.
 - If content is contained on pupils personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
- immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a pupil has been exposed to CSAM we will:
 - ensure that the DSL is informed urgently so appropriate safeguarding action/support can be taken/provided in line with our child protection policy.
 - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or to the police.
 - inform the police as appropriate, for example if images have been deliberately sent to or shared by pupils.
 - report concerns as appropriate to parents and carers.
- If made aware that CSAM has been found/viewed on school provided networks/devices, we will:
 - ensure that the DSL is informed urgently so appropriate safeguarding action/support can be taken/provided in line with our child protection policy.
 - 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 any other agencies, 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 has viewed or is in possession of CSAM, we will:
 - quarantine any involved school provided devices/network access until police advice has been sought.
 - ensure that the headteacher is informed in line with our managing allegations against staff policy.
 - inform the LADO and other relevant organisations, such as the police, in accordance with our managing allegations against staff policy.

11.2.5 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Chilton Primary 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.
- Crimes committed against someone because of their disability, transgender-identity, race, religion or belief, or sexual orientation are hate crimes and can be reported to the police via 101, 999 (if someone is in immediate danger) or via https://www.report-it.org.uk/your_police_force
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Local Authority and/or the police.

11.2.6 Online radicalisation and extremism

- As per section 7 of this policy, we will take all reasonable precautions to ensure that **pupil** and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are made aware of online material promoting terrorism or extremism, we will report it to the Home Office via If we are made aware of online material promoting terrorism or extremism, we will report it via <https://www.gov.uk/report-terrorism>
- If we are concerned that a child or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with our child protection, staff code of conduct and allegations policies.

11.2.7 Cybercrime

- Chilton Primary School recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into ‘cyber-enabled’ (crimes that can happen offline but are enabled at scale and at speed online) or ‘cyber dependent’ (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the [Cyber Choices](#) programme, which aims to intervene when children are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.
- Where there are concerns about ‘cyber-enabled’ crime such as fraud, purchasing of illegal drugs online, child sexual abuse and exploitation, or other areas of concern such as online bullying or general online safety, they will be responded to in line with our child protection policy and other appropriate policies.
- Children who are affected by cybercrime will be supported in line with our safeguarding and pastoral support systems.

11.3 Responding to content or activity online that may be inappropriate

- Inappropriate content refers to material that is illegal, harmful, or unsuitable for children. This includes, but is not limited to, pornography, content that encourages, promotes or provides instructions for self-harm, suicide or eating disorders, abusive or hateful content, content which depicts or encourages serious violence or injury, content which encourages dangerous stunts and challenges, and content which encourages the ingestion, inhalation or exposure to harmful substances.
- The DSL holds overall responsibility for online safety and will respond to concerns regarding content or activity online that may be inappropriate in line with the school’s Child Protection, Online Safety, Behaviour, Anti-Bullying, and Acceptable Use policies.
 - All staff must be aware of the procedures for identifying, recording, and reporting incidents involving inappropriate activity or content. This includes activity or content accessed via school-owned devices, personal devices used on-site, or content shared between pupils or staff.
 - Pupils should report any exposure to inappropriate activity or content to a trusted adult.
- The DSL will assess the concern and determine the appropriate response, which may include:

- Internal sanctions or support in line with our Child Protection, Online Safety, Behaviour, Anti-Bullying, and/or Acceptable Use policies.
- Engagement with parents/carers.
- Referral to external safeguarding partners or law enforcement as appropriate.

12. Useful Links

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- South West Grid for Learning (SWGfL): 360 Safe Self-Review tool for schools www.360safe.org.uk
- London Grid for Learning: <https://lgfl.net/safeguarding>
- 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
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: <https://educateagainsthate.com>
- NCA-CEOP Education Resources: www.ceopeducation.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org
- IWF/NCA Responding to AI Generated CSAM: www.iwf.org.uk/resources/ai-generated-child-sexual-abuse-material-professionals-resource/
- Centre of expertise on child sexual abuse: <https://www.csacentre.org.uk/research-resources/practice-resources/>

Reporting and Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
 - Report Remove Tool for nude images: [www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online](http://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety sexting/report-nude-image-online)
- NCMEC Take it down: <https://takeitdown.ncmec.org/>
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: <https://reportharmfulcontent.com>
- Revenge Porn Helpline: <https://revengepornhelpline.org.uk>
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- Papyrus: www.papyrus-uk.org/
- NCA CyberChoices: www.nationalcrimeagency.gov.uk/cyber-choices

Support for children and parents/carers

- Internet Matters: www.internetmatters.org

- Childnet: www.childnet.com
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parents Protect: www.parentsprotect.co.uk
- NCA-CEOP Child and Parent Resources: www.ceopeducation.co.uk
- Parent Zone: <https://parentzone.org.uk>
- Get Safe Online: www.getsafeonline.org
- Common Sense Media: www.common sense media.org
- Samaritans: www.samaritans.org/about-samaritans/research-policy/internet-suicide/
- Shore Space: <https://shorespace.org.uk/>