

GREAT CHART PRIMARY SCHOOL

ONLINE SAFETY POLICY

September 2023



A Great Place to Discover and Learn

Vision Statement

A respectful community where we thrive and achieve our full potential as confident life long learners

Mission Statement

Preparing for life in our ever changing world, by providing opportunities to develop core values and a love of learning

Our core value is Respect

Our termly values: Team work, Ambition, Responsibility, Resilience, Kindness & Independence

Great Chart Primary School Online Safety Policy

Key Details

Designated Safeguarding Lead (s): ([Wendy Pang](#), [Paula High](#), [Jo Adams](#), [Sarah Cadman](#), [Nicky Ostridge](#), [Torie Davies \(EYFS\)](#))

Named Governor with lead responsibility: ([Mr Ronnie Manek](#))

Date written: (September 2023)

Date agreed and ratified by Governing Body: (October 2023)

Date reviewed: (September 2024)

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

Great Chart Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Great Chart Primary School involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance [‘Keeping Children Safe in Education’](#) 2022, [Early Years and Foundation Stage](#) 2021 [‘Working Together to Safeguard Children’](#) 2022, [Education for a Connected World](#) 2020 and the [Kent Safeguarding Children Multi-agency Partnership](#) (KSCMP) procedures.
- The purpose of the Great Chart online safety policy is to:
 - Safeguard and protect all members of the Great Chart community online.
 - Identify approaches to educate and raise awareness of online safety throughout the community.
 - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns.
- We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all learners 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 learners and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.
- Great Chart School understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
 - **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
 - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
 - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

- o **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- Great Chart 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 their peers online.
- This policy applies to learners, 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).
- Great Chart School identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.
- This policy links with several other policies, practices and action plans, including but not limited to:
 - o Anti-bullying policy
 - o Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
 - o Behaviour and discipline policy
 - o Child protection policy
 - o Confidentiality policy
 - o Data protection
 - o Data/information security
 - o Cameras and image use policy
 - o Mobile and smart technology

Responding to Emerging Risks

- Great Chart School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
 - o 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 learners face.
 - o regularly review the methods used to identify, assess and minimise online risks.
 - o examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
 - o ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
 - o 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. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Jo Adams) has lead responsibility for online safety.
- Great Chart Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

3.1 The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

3.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.

- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

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

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

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team and the IT Support.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

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

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

3.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use our systems, such as Google Classroom, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement Approaches

4.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study. *(All pupils to follow [Project Evolve from September 2020](#))*
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology.
 - Implementing appropriate peer education approaches.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
 - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.
 - Great Chart Primary School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
 - displaying acceptable use posters in all rooms with internet access.
 - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
 - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
 - Great Chart Primary School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
 - ensuring age appropriate education regarding safe and responsible use precedes internet access.
 - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
 - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
 - enabling them to understand what acceptable and unacceptable online behaviour looks like.

- preparing them to identify possible online risks and make informed decisions about how to act and respond.
- ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

4.2 Vulnerable Learners

- Great Chart recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Great Chart will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners if needed.
- When implementing an appropriate online safety policy and curriculum Great Chart will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher. (*Paula High*)

4.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates in our Visioning Day. This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

4.4 Awareness and engagement with parents and carers

- Great Chart recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

- We will build a partnership approach to online safety with parents and carers by:
 - Providing information and guidance on online safety in a variety of formats.
This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings and transition events.
 - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
 - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
 - Requiring them to read our acceptable use policies and discuss the implications with their children.

5. Reducing Online Risks

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

6. Safer Use of Technology

6.1 Classroom Use

- Great Chart uses a wide range of technology. This includes access to:
 - Computers, chromebooks, ipads, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - Google Apps for Education
 - Email
 - Games consoles and other games-based technologies
 - Digital cameras and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- Only staff have access to download free apps, any paid apps need to be installed by the school IT technician.
 - Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
 - The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
 - We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
-
- Supervision of learners will be appropriate to their age and ability.
 - **Early Years Foundation Stage and Key Stage 1**
 - Access to the internet will be by adult demonstration, as well as directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
 - **Key Stage 2**
 - Learners will use age-appropriate search engines and online tools or be taught how to search safely using keywords.
 - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.
 - Teachers should check any websites used in lessons prior to the lesson.

6.2 Managing Internet Access

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

7 Filtering and Monitoring

7.1 Decision Making

- Great Chart School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- Great Chart School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances. Our Technical Support has looked at all options available.

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

7.2 Filtering

- Education broadband connectivity is provided through Broadband 4.
- We use [Relay through Broadband 4](#), our internet provider, which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- We work to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
 - **If on a desktop computer the screen must be switched off, if on a chromebook the lid must be put down and if on an ipad the ipad must be turned over.**
 - The member of staff will report the concern (including the URL of the site if possible) to the DSL Online Safety Officer and technical staff.
 - The breach will be recorded and escalated as appropriate.
 - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

7.4 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
 - ***This will be through physical monitoring (supervision) and monitoring internet and web access.***
 - ***We have now purchased a programme that allows us to monitor websites children access at school. This is being trialled in Year 6 and then rolled out across the school.***
- If a concern is identified via monitoring approaches we will:
 - ***Complete a report of the incident on the CPOMS system and the Online Safety Officer will be alerted to these.***
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.5 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
 - Full information can be found in our information security policy.

7.6 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly.
 - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
 - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on our network,
 - The appropriate use of user logins and passwords to access our network.
 - Specific user logins and passwords will be enforced for all but the youngest users. (EYFS and KS1)
 - 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.

7.7 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 4, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private. In Year 1, 2 and 3 passwords are generic but access is limited within our setting.
- We require all users to:
 - Use strong passwords for access into our system.
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.

7.8 Managing the Safety of our Website

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

7.9 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/behaviour, social media and use of personal devices and mobile phones.

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 policies and the code of conduct/behaviour policy.
 - The forwarding of any chain messages/emails is not permitted.
 - Spam or junk mail will be blocked and reported to the email provider.
 - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
 - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell Online Safety Lead if they receive offensive communication, and this will be recorded on our safeguarding system.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
 - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.
- Staff must only email between the hours of 7.30am and 9.30pm.

8.2 Learner email

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

8.3 Management of Learning Platforms

- Great Chart uses Google for Education as its official learning platform. The children use Google Classroom.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff *and/or* learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive.
 - If the user does not comply, the material will be removed by the site administrator.
 - Access to the LP for the user may be suspended.
 - The user will need to discuss the issues with a member of leadership before reinstatement.
 - A learner's parents/carers may be informed.
 - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

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

- We use Arbor to track learners progress and share appropriate information with parents and carers. In the Early Years Foundation Stage we use Tapestry.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
 - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.

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

9. Social Media

9.1 Expectations

- The policy applies to all use of social media; the term social media includes, but is 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.
- The expectations' regarding safe and responsible use of social media applies to all members of Great Chart Primary School community.
- All members of Great Chart Primary School community are expected to engage in social media in a positive, safe and responsible manner.
 - All members of Great Chart Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
 - The use of social media during setting hours for personal use is permitted.
 - **(Staff may access at break and lunchtimes only)\.**
 - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Great Chart Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
 - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - Setting the privacy levels of their personal sites.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Great Chart Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct/behaviour policy and/or 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.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
 - Any pre-existing relationships or exceptions that may compromise this, will be discussed with the headteacher.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted. Staff may reply to parents via the Google Classroom or school email address if they are happy to do so. If not they must ask parents to contact them via the school office.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL.

9.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
 - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
 - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications.
 - How to report concerns both within the setting and externally.

9.4 Official Use of Social Media

- Great Chart Primary School official social media channels are:
 - <https://www.youtube.com/channel/UCmFFgqnx69iumuhyAek8hQQ> and Facebook as well as Class Dojo.
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.

- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use setting provided email addresses to register for and manage any official social media channels.
 - Official social media sites are suitably protected and, where possible, linked to our website.
 - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents and carers will be informed of any official social media use with learners; any official social media activity involving learners 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.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
 - Always be professional and aware they are an ambassador for the setting.
 - Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the setting.
 - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
 - Ensure that they have appropriate consent before sharing images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
 - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
 - Inform their line manager, the DSL, of any concerns, such as criticism, inappropriate content or contact from learners.

11. Use of Mobile and Smart Technology

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

11.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
 - All members of Great Chart Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - All members of Great Chart Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of Great Chart Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

11.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, staff behaviour/code of conduct and Acceptable Use Policies.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place e.g. locked in a drawer or kept in a bag during lesson time.
 - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.

- Not use personal devices during teaching periods unless written permission has been given by the headteacher, such as in emergency circumstances.
 - Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
 - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and/or headteacher.
- Staff will only use school provided equipment (not personal devices):
 - to take photos or videos of learners in line with our image use policy.
 - to work directly with learners during lessons/educational activities.
 - to communicate with parents/carers.
- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or remote learning AUP.
- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

11.3 Learners Use of Personal Devices and Mobile Phones/Smart Watches

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Great Chart Primary School expects learners' personal devices (only applicable to Year 6 children) and mobile phones to be kept in their bag.
- Smart watches are not allowed for any reason at Great Chart School as they can cause a distraction to pupils.
- Even when apparently silent, the notifications on smart watches could distract pupils from their learning.
- Use of smart watches with integrated cameras could lead to child protection and data protection issues with regard to inappropriate capture, use, or distribution of images.
- If a learner needs to contact his/her parents or carers during the school day they will be allowed to use the office phone. Parents are advised to contact their child via the setting office.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.

- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
- If a child has used a mobile phone in school (in breach of the Mobile Phone Agreement) then they will no longer be able to bring their phones to school until further notice.

11.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of our policy.

11.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

12.Responding to Online Safety Incidents and Concerns

12.1 Online child on child abuse

- Great Chart School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- 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

- o sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
- o consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
- o 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
- o 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
- o initiation/hazing type violence and rituals.
- Great Chart School believes that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as “banter”, “just having a laugh”, “part of growing up” or “boys being boys” as this can lead to a culture of unacceptable behaviours and an unsafe environment for children.
- Great Chart School believes that all staff have a role to play in challenging inappropriate online behaviours between peers.
- Great Chart 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.
- Concerns about learner's behaviour, including child on child abuse taking place online offsite will be responded to as part of a partnership approach with learners and parents/carers and in line with existing policies, for example anti-bullying, acceptable use, behaviour and child protection policies. **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 e.g. when children are not under the lawful control or charge of a member of school staff, to such extent as is reasonable. This legislation is not applicable to independent schools.**
- Great Chart want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online peer on peer 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. Learners who experience abuse will be offered appropriate support, regardless of where the abuse takes place.
- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content. In the first instance staff must report using the CPOMS system.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
 - o Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL will speak with Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

12.1 Concerns about Learners Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL will record these issues in line with our child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

12.2 Concerns about staff online behaviour and/or welfare

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

12.3 Concerns about parent/carers online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher and/or DSL (or deputy). They will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

13. Procedures for Responding to Specific Online Incidents or Concerns

13.1 Nude or semi-nude image sharing

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. The UKCIS '[Sharing nudes and semi-nudes: advice for education settings working with children and young people](#)' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing, and should be read and understood by DSLs working with all age groups, not just older learners.

- Great Chart 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") can be 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:
 - o creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
 - o 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.
 - o 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, Great Chart 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](#)'
- Great Chart 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:
 - o Report any concerns to the DSL immediately.
 - o Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.

- o Not delete the imagery or ask the child to delete it.
- o Not say or do anything to blame or shame any children involved.
- o 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.
- o Not ask the child or children involved in the incident to disclose information regarding the imagery and 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:
 - o act in accordance with our child protection policies and the relevant local procedures and in line with the [UKCIS](#) guidance.
 - o carry out a risk assessment in line with the [UKCIS](#) guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
 - o 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.
 - o The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
 - o If DSLs are unsure how to proceed, advice will be sought from the local authority.
 - o Store any devices securely:
 - If content is contained on learners' personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
 - o 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.
 - o provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
 - o 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.
 - Learners 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 learners to do so.

13.2 Online Sexual Violence and Sexual Harassment between Children

- Our Headteacher, DSL and appropriate members of staff have accessed and understood the DfE “[Sexual violence and sexual harassment between children in schools and colleges](#)” (2018) guidance and part 5 of ‘[Keeping children safe in education](#)’ 2022.
 - Full details of our response to child on child abuse, including sexual violence and harassment can be found in our child protection policy.
- Great Chart School recognises that sexual violence and sexual harassment between children can take place online. Examples may include;
 - Non-consensual sharing of sexual images and videos
 - Sexualised online bullying
 - Online coercion and threats
 - ‘Upskirting’, which typically involves taking a picture under a person’s clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
 - Unwanted sexual comments and messages on social media
 - Online sexual exploitation
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
 - immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
 - if content is contained on learners personal devices, they will be managed in accordance with the DfE ‘[searching screening and confiscation](#)’ advice.
 - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
 - implement appropriate sanctions in accordance with our behaviour policy.
 - inform parents and carers, if appropriate, about the incident and how it is being managed.

- If appropriate, make referrals to partner agencies, such as Children's Social Work Service and/or the police.
- If the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
 - If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Great Chart Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Great Chart Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Great Chart 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum. We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

13.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Great Chart Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Great Chart Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. This is available on our website and children will be educated about when they need to use it.

- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
 - Act in accordance with our child protection policies and the relevant Kent Safeguarding Children's Board's procedures.
 - If appropriate, store any devices involved securely.
 - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
 - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
 - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](#) (CSET) by the DSL.
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

13.4 Indecent Images of Children (IIOC)

- Great Chart Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If it is unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - Ensure that the DSL is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
 - Ensure that the DSL is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
 - Ensure that the headteacher is informed in line with our managing allegations against staff policy.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
 - Quarantine any devices until police advice has been sought.

13.5 Cyberbullying

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

13.6 Online Hate

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

13.8 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL 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 the child protection and allegations policies.

13.9 Cybercrime

- Great Chart 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 young people 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.

Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings

Education Safeguarding Team:

Kent Educational Setting Support and Guidance

Education Safeguarding Service, The Education People:

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

KSCMP: www.kscb.org.uk

Kent Police:

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

Front Door:

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

Early Help and Preventative Services:

www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

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

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

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

- Internet Watch Foundation (IWF): www.iwf.org.uk
- UK Council for Internet Safety (UKCIS):
www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
 - Report Harmful Content: <https://reportharmfulcontent.com/>
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Childnet: www.childnet.com
 - Step Up Speak Up – Online Sexual Harassment Guidance:
www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
 - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- Internet Matters: www.internetmatters.org
- Parent Zone: <https://parentzone.org.uk>
- Parent Info: <https://parentinfo.org>
- NSPCC: www.nspcc.org.uk/online-safety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Get Safe Online: www.getsafeonline.org

See Flowchart below for further clarification.

Disclaimer

The Education People make every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable.

The copyright of these materials is held by The Education People. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not for profit use, providing the Education People copyright is acknowledged and we are informed of.