Online Safety Policy

Governor Review Date	Autumn 2020
Review Frequency	Annual
Date for Next Review	Autumn 2021
Head Teacher Approval	Autumn 2020
Governor Approval	3rd February 2021

Creating an Online Safety Ethos

Aims and Policy Scope

Caedmon Primary School believes that Online Safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Caedmon Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Caedmon Primary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Caedmon Primary School's Online Safety Policy is to:

- Clearly identify the key principles expected of all members of the school community with regards to the safe and responsible use of technology to ensure that school is a safe and secure environment.
- Safeguard and protect all members of Caedmon Primary School's community online.
- Raise awareness with all members of Caedmon Primary School's community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

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

This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding and Child Protection, Anti-Bullying, Behaviour, Staff Code of Conduct, Acceptable Use Policies.

Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) and Online Safety Lead is Mr P Wiley.

The Designated Safeguarding Governor is Mr S Goldswain.

The policy has been approved and agreed by the Governing Body.

The Online Safety (e–Safety) Policy and its implementation will be reviewed by the school at least annually or sooner if required.

Key responsibilities for the community:

The key responsibilities of the Online Safety Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms.
- Monitor the school online safety incidents to identify gaps/trends and use this data to update the school education response to reflect need.
- To report to the Senior Leadership Team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership and management to review and update the Online Safety Policy, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

The key responsibilities of the Senior Leadership Team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.

- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that staff risk assess the safe use of technology, including ensuring the safe and responsible use of devices.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.

The key responsibilities for all members of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site. Please see the Code of Conduct and Social Networking Policy for further information.

- Demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area.
- Staff receive regular information and training on online safety and how they can promote a message of 'stay safe' to the children they work with. New staff receive a copy of this policy and of the AUP as part of their induction.

In addition to the above, the key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the Local Authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and Senior Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school's Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.

- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

The key responsibilities of parents and carers are:

- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the school's Online Safety Policy.
- Using school systems, such as learning platforms and school approved social media, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

Online Communication and Safer Use of Technology

Managing the school website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).

The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The Head Teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

Pupils' work will be published with their permission or that of their parents/carers.

The administrator account for the school website will be safeguarded with an appropriately strong password.

The school will post information about safeguarding, including online safety, on the school website for members of the community.

Publishing images and videos online

The school will ensure that all use of images and videos take place in accordance other policies and procedures including, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.

In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

Managing email

Use of email

Staff will be given a "professional" email account. The account is set up using the Microsoft Outlook Web Access. The staff are at liberty to use their accounts for correspondence between one another or other professional bodies as part of their work. Passwords must be changed by the user. Users agree through the staff agreement form to keep passwords secret, even from their family and friends.

- Pupils may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school email address to use for any official communication. This account should be used for all school business.
- The use of personal email addresses by staff for any official school business is not permitted. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider. Staff must inform the Online Safety Lead/Designated Safeguarding Lead if they receive an offensive email
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Whole -class or group email addresses may be used for communication outside of the school
- Staff will be encouraged to develop an appropriate work life balance when responding to email. There is no expectation for staff to access their work emails after their contracted working hour or over a weekend, although staff will access emails at an appropriate time during the day to check for any updates. However staff access their school email, all the school email policies apply.
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.

- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Appropriate and safe classroom use of the internet and any associated devices

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum documents for further information.

The school's internet access will be designed to enhance and extend education.
Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.

Supervision of pupils will be appropriate to their age and ability.

At Early Years Foundation Stage and Key Stage 1, pupils' 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.

At Key Stage 2, pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.

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

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will use age appropriate search tools as decided by the class teacher.

The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

All accidental internet incidents involving pupils and/or staff must be reported immediately to the administration staff at Caedmon Primary. The parents of children involved should also be informed.

Social Media

Expectations regarding safe and responsible use of social media will apply to all members of Caedmon Primary School's community and exist in order to safeguard both the school and the wider community, on and offline. See the Social Networking Policy for further information.

Caedmon Primary School's official social media channels are: ***@CaedmonPS on Twitter and @CaedmonPri on Facebook.***

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including Anti-Bullying and Safeguarding and Child Protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the school Image Use Policy.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorized to do so.
- Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Head Teacher of any concerns such as criticism or inappropriate content posted online.

- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.

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. See the Social Networking Policy for further information.

- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including Child Protection Policy and Procedures, Anti-Bullying and Behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

Use of Personal Devices and Mobile Phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of Caedmon Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use Policy and Code of Conduct.

Caedmon Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools.

Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school. Members of staff should only use them during working hours during a designated break period inside of the staff room. Mobile phones and personal devices should be stored in the member of staff's allocated locker. All visitors to school are required to store their phone in a locker, unless being supervised by a member of staff (e.g. multi agency meeting) or otherwise agreed with the Headteacher or Designated Safegurding Lead for a specific reason (e.g. social care, police officers etc). In this instance, mobile phones should be turned off and not used until in a designated area.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Child Protection Policy and Procedures, Online Safety Policy, Acceptable Use Policy and Behaviour Policy.
- All members of Caedmon Primary School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of Caedmon Primary School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential.
- All members of Caedmon Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school policies.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies
- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. Code of Conduct, Acceptable Use etc.

- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances. Any mobile phone usage must take place in a designated area (e.g. staffroom).
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- 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 then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school's policies.

Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Mobile phones and devices are not permitted within school and should be handed to the class teacher immediately if one is brought into school.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Anti-Bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership Team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy. (***See*** https://www.gov.uk/government/publications/searching-screening-and-confiscation ***)***
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's Acceptable Use Policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school Image Use Policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

Reducing online risks

- Caedmon Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. The school's 100Mb broadband connection is provided by OneIT. The filters at each stage are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. However, when dealing with the internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined below have been taken. Use of the web through the OneIT link is monitored and traceable by OneIT network administrators. In addition to this is the consideration that children will inevitably access the internet outside of school. We therefore aim to educate them about internet safety, not simply cover their eyes.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the Online Safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the Senior Leadership Team.

Internet use throughout the wider school community

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with children with Special Educational Needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Engagement and education of children and young people

- An Online Safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Online Safety (e-Safety) will be included in the wider curriculum, covering both safe school and home use.
- Acceptable Use expectations and posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal Online Safety (e-Safety) education approaches.
- The school will reward positive use of technology by pupils.
- We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any Internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas. We will teach children how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- Children will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- When searching the Internet for information, search engines will be set to 'Safe Search' so that only appropriate content is accessed. All use will be monitored and students will be reminded of what to do, if they come across unsuitable content.

- Children will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Children will be made aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Engagement and education of children and young people considered to be vulnerable

Caedmon Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors. As a school, we will ensure that differentiated and ability appropriate Online Safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

Engagement and education of staff

- The Online Safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- Up-to-date and appropriate staff training/guidance in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The school will highlight useful online tools which staff should use according to the age and ability of the pupils.

Engagement and education of parents and carers

- Caedmon Primary School recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school Online Safety (e-Safety) policy and expectations and other relevant information in newsletters, letters and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.

- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.

Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
Full information regarding the school's approach to data protection and information governance can be found in the Data Protection Policy.

Passwords

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.

Filtering and Monitoring

- The governors will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit children's exposure to online risks.
- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
- All monitoring of school owned/provided systems will take place to safeguard members of the community.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
- If pupils discover unsuitable sites, the URL will be reported to the class teacher and will then be recorded and escalated as appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as the Police, Child Exploitation and Online Protection Centre (CEOP) and the Internet Watch Foundation (IWF) immediately.

- If you find an appropriate web site that you would like to use in school for educational purposes and you have viewed it to ensure its suitability, you may request to have it unblocked.
- You can email the IT helpdesk to request this at: helpdesk@oneittss.org.uk

Management of applications (apps) used to record children's progress

- The Headteacher is ultimately responsible for the security of any data or images held of children.
- Apps/systems which store personal data will be risk assessed prior to use.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.
- Parents will be informed of the school's expectations regarding safe and appropriate use (e.g. not sharing passwords or sharing images) prior to being given access.

Responding to Online Incidents and Safeguarding Concerns

- All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for pupils.
- All members of the school community will be informed about the procedure for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies.
- Complaints about Internet misuse will be dealt with under the school's Complaints Policy.
- Complaints about online/cyber bullying will be dealt with under the school's Anti-Bullying Policy.
- Any complaint about staff misuse will be referred to the Head Teacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the school's complaints procedure.

- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- The school will manage online safety (e-Safety) incidents in accordance with the Behaviour Policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the First Contact Team (01642 130700) or the Police via 101 or 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the First Contact Team.
- If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the First Contact Team to communicate to other schools.
- Parents and children will need to work in partnership with the school to resolve issues.

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns
Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting".

Caedmon Primary School ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
Caedmon Primary School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance.

If the school are made aware of incidents involving creating youth produced sexual imagery the school will:

- Act in accordance with the school's Child Protection and Safeguarding Policy and Procedures and the relevant Local Safeguarding Child Boards procedures.
- Immediately notify the Designated Safeguarding Lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the school's Behaviour Policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the Senior Leadership Team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.

The school will not view an image suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).

The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.

If an indecent image has been taken or shared on the school's network or devices then the school will take action to block access to all users and isolate the image.
The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.

The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- Caedmon Primary School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
- Caedmon Primary School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the First Contact Team and/or the Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the First Contact team by the DSL.
- If the school are made aware of incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the school's Child Protection and Safeguarding Policy and Procedures and the relevant Local Safeguarding Child Boards procedures.
    - Immediately notify the Designated Safeguarding Lead.
    - Store any devices involved securely.
    - Immediately inform police via 101 (using 999 if a child is at immediate risk).
    - Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care (if needed/appropriate).
    - Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school Leadership Team will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.
- If pupils at other schools are believed to have been targeted then the school will seek support from the First Contact Team to enable other schools to take appropriate action to safeguarding their community.
- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button on the school website.

Responding to concerns regarding Indecent Images of Children (IIOC)

Caedmon Primary School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

- The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the First Contac Team and/or the Police.
- If the school is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the schools Child Protection Policy and the relevant Local Safeguarding Child Boards procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
  - Ensure that the Designated Safeguard Lead is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  -

- If the school are made aware that indecent images of children have been found on the school's electronic devices then the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy. Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the First Contact Team and/or the Police.

Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of Caedmon Primary School community will not be tolerated. Full details are set out in the school policies regarding Anti-Bullying and Behaviour. All incidents of online bullying reported will be recorded. There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the First Contact Team and/or the Police.
Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence. The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary. Pupils, staff and parents/carers will be required to

work with the school to support the approach to cyberbullying and the school's Online Safety ethos.

Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's Anti-Bullying, Behaviour Policy or Acceptable Use Policy.
- Parent/carers of pupils involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

Responding to concerns regarding online hate

Online hate at Caedmon Primary School will not be tolerated.
All incidents of online hate reported to the school will be recorded.
All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. Anti-Bullying, Behaviour etc.
The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the First Contact Team and/or the Police

Appendix B

Online Safety (e-Safety) Contacts and References

National Links and Resources
Action Fraud: www.actionfraud.police.uk
BBC WebWise: www.bbc.co.uk/webwise
CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
ChildLine: www.childline.org.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
Know the Net: www.knowthenet.org.uk
Net Aware: www.net-aware.org.uk
NSPCC: www.nspcc.org.uk/onlinesafety
Parent Port: www.parentport.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/
Think U Know: www.thinkuknow.co.uk
Virtual Global Taskforce: www.virtualglobaltaskforce.com
UK Safer Internet Centre: www.saferinternet.org.uk
360 Safe Self-Review tool for schools: https://360safe.org.uk/
Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

Searching, Screening and Confiscation:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf
UK Council For Internet Safety: https://www.gov.uk/government/organisations/uk-council-for-internet-safety