Online Safety Policy



The school has a Designated Online Safety Leader (Richard Bridge), who is responsible for reviewing and updating this policy. They work in collaboration with members of the SLT in order to ensure this policy meets the ever-changing issues relating to the internet and its safe use.

The Online Safety Policy has been written by the school, incorporating points from the Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education', its non-statutory guidance 'Teaching Online Safety in Schools' and a number of other carefully selected sources. Key documents in school that inform this document and have, in turn, been informed by this document include the Steel River Academy Trust Safeguarding Policy and the Caedmon Child Protection and Safeguarding Policy. This policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly and updated at least annually. Changes will be made immediately if technological or other developments require it.

<u>Online Safety Risks</u>

The Department for Education published an updated version of 'Keeping children safe in education' in 2026. It states the following:

Review Date	**September 2026**
Review Frequency	**Annually**
Date for Next Review	**September 2027**
Author	**R.Bridge**
Governor Approval	**Autumn 2026**

1. *All staff should be aware of the indicators of abuse, and neglect and exploitation (see below), understanding that children can be at risk of harm inside and*

outside of the school/college, inside and outside of home, and online. Exercising professional curiosity and knowing what to look for is vital for the early identification of abuse and neglect so that staff are able to identify cases of children who may be in need of help or protection.

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.

2. *It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.*

3. *The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:*

3.1 *content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.*

3.2 *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.*

3.3 *conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and*

3.4 *commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

At Caedmon Primary School, we also recognise these recent yet relevant developments in each aspect of risk:

Content risks also include the possibility that children can be exposed to emerging risks such as AI-generated harmful content and manipulated or synthetic media such as deepfakes.

Contact also includes interactions through AI-powered chatbots, virtual companions or other emerging technologies that may facilitate grooming, exploitation or harmful influence.

Conduct also includes creating or sharing AI-generated intimate images or deepfakes, online bullying, harassment, image-based abuse, coercion and exploitation.

Commerce also includes fraudulent online activity and exploitation through online platforms.

The KCSIE document for 2026 includes aligning the definition of safeguarding used with that in Working Together to Safeguard Children (2023). This makes explicit reference to online activity:

3.5 *No single practitioner can have a full picture of a child's needs and circumstances. If children and families are to receive the right help at the right time, everyone who comes into contact with them has a role to play in identifying concerns, sharing information and taking prompt action. Safeguarding and promoting the welfare of children is defined for the purposes of this guidance as:*

• *Providing help and support to meet the needs of children as soon as problems emerge*

• *protecting children from maltreatment,* ***whether that is within or outside the home, including online***

• *preventing the impairment of children's mental and physical health or development*

• *ensuring that children grow up in circumstances consistent with the provision of safe and effective care*

• *taking action to enable all children to have the best outcomes.*

Furthermore, the importance of staff understanding the role that children can play in abusing other children is highlighted in the document:

4. *All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school or college and*

online. All staff should be clear as to the school or college's policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

More detail on this matter is included in the school's Child Protection & Safeguarding Policy.

The following sections of this policy address the above risks and the systems in place to reduce the risk both within school and for our children in their home lives.

Filters and monitoring

Statutory guidance from the 2026 update of KCSIE dictates the following:

5. *Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.*

Filtering and monitoring expectations in schools and education settings have been updated in the document 'Meeting digital and technology standards in schools and colleges':

6. *The Department for Education's filtering and monitoring standards set out that schools and colleges should:*

- *identify and assign roles and responsibilities to manage filtering and monitoring systems.*
- *review filtering and monitoring provision at least annually.*
- *block harmful and inappropriate content without unreasonably impacting teaching and learning.*
- *have effective monitoring strategies in place that meet their safeguarding needs.*

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Additional guidance on "appropriate" filtering and monitoring can be found at: UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/teachersand-school-staff/appropriate-filtering-and-monitoring. The UK Safer Internet Centre produced a series of webinars for teachers on behalf of the Department. These webinars were designed to inform and support schools with their filtering and monitoring responsibilities and can be assessed at Filtering and monitoring webinars available – UK Safer Internet Centre. South West Grid for Learning (swgfl.org.uk) has created a tool to check whether a school or college's filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content).

7. *Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology, which will also reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

In line with DfE guidance, the school has appropriate filtering and monitoring systems in place. The school's broadband connection is provided by OneIT. The filters in place are extensive and include lists of illegal sites/inappropriate sites that cannot be accessed. It also allows open access and sharing of resources between educational establishments. Use of the internet through OneIT's services is monitored and traceable by the network administrators, including alerts provided to the DSL (Mrs Marsden) in the event of access to websites that may contain inappropriate content. In addition to this, there is the consideration that children will inevitably access the internet outside of school. It is therefore vital that we give our children the tools and knowledge to empower them to be safe on the internet and equally as important - to know what to do when they come across any of the dangers. This is addressed further below.

From time-to-time, websites can be blocked even though there are no obvious threats or dangers. Once these have been checked thoroughly by a member of staff, they can contact the OneIT Helpdesk to notify them that a website is suitable for educational purposes. This can be done at: https://portal.oneitss.org.uk/#/. Staff have account log in details for this purpose.

Searches using the school's network are monitored. The school uses Securly to notify the headteacher of any inappropriate searches or searches which then result in accessing a site with potentially inappropriate content. The headteacher will then follow up any of these breaches and a log is held in the office.

In 2024, the DfE also provided an update entitled 'Cyber security standards for schools and colleges'. This is relevant here as it references 'safeguarding issues due to sensitive personal data being compromised' and states:

The cyber security standards have been updated to address tasks that should be completed by both the senior leadership team (SLT) and IT support. Cyber security is not something that IT teams can carry out alone, it is a shared responsibility between multiple roles and teams.

In addition, the 2026 update of KCSIE includes reference to the Department for Education's guidance on generative AI, 'Generative AI: product safety expectations' (2025). This highlights emerging risks linked to generative artificial intelligence (AI), including AI-generated images, deepfakes, 'nudification' technology and AI-enabled harassment or exploitation. The school recognises that AI tools may be used in ways that cause harm, facilitate bullying, create or manipulate images without consent, spread misinformation or generate inappropriate content. Staff will remain vigilant to these risks and will address them through safeguarding procedures, online safety education and appropriate filtering and monitoring systems.

Further guidance regarding the educational use of artificial intelligence is contained within the school's AI Policy.

Online Safety Training for Staff and Governors

At Caedmon Primary School we ensure that all teaching and non-teaching staff can recognise and are aware of Online Safety issues. All staff take responsibility for promoting online safety. The 2026 update to KCSIE states:

8*. Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description.*

Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction. This training should equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding. Their training should be updated regularly.

Annual training and updates have been delivered previously by Simon Finch, a leader in safeguarding and digital literacy. In February 2023, Stacey Coates completed the CEOP Ambassador training course and attended further CEOP training conferences annually. She has provided staff training since then. Staff training will also include emerging Online Safety risks, including artificial intelligence (AI), deepfakes, AI-generated imagery, misinformation and disinformation, image-based abuse, online harassment and other developing technologies that may impact safeguarding. AI-specific training will also be referenced in the Trust's Artificial Intelligence Use and Teaching policy.

In addition to this, staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding (for example, the Prevent strategy). They are also directed to relevant websites to help support their understanding of these issues. All members of staff are also aware of the documents and policies which must be updated throughout each year and where their actions need to be monitored and logged (see Managing Online Safety in School below). During September, each member of staff reviews the policies for both Online Safety and Acceptable Use and they also review the statements which underpin their Acceptable Use Agreement and Staff Code of Conduct Policy.

Online Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive online safety education and information (e.g. via the school website, Facebook and ParentMail) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good online safety behaviour. Each year, 'Parent Welcome' meetings are set up each September to invite parents in to discuss what they should expect over the coming academic year. At these meetings, a member of staff delivers a short Online Safety presentation on the issues surrounding staying safe online. These meetings include valuable information which includes; cyberbullying, password safety, social networking sites and the use of other gaming media. The school also subscribe to updates from National Online Safety created by The National College which are shared in the form of PDF guides for parents. These guides focus on recent changes in technology, new or updated versions of games or apps or concerning issues that could affect children and young people. These are shared weekly with parents via ParentMail to ensure they are kept informed of the latest developments.

Online Safety within the Curriculum

With regard to teaching Online Safety in school, the 2026 KCSIE update states:

9. Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities (SEND).

Using searchable cached sites such as Discovery/Espresso provide a completely safe environment for children to conduct research. However, limiting access will not protect children and educate them to be safe on the internet. Therefore, it is vital to provide opportunities for children to conduct safe searches.

During any lesson which involves children using the internet, tasks and expectations will be made explicit to children to ensure they aware of what they are and are not allowed to do.

Children will not be allowed to access and search the internet unless authorised by a member of staff. Responsibility for the monitoring of what the children find is then the responsibility of that adult. Details of when the use of searching on the internet is appropriate can be found in the school scheme of work for computing; other uses are the sole responsibility of the supervising adult.

Accessing and interacting with the internet is a key aspect of many users' reasons for having an internet connection. Simply preventing the children from using internet is not preparing them for the real world (including for use at home). Therefore,

Online Safety is implicitly taught throughout school and referred to whenever a unit of work requires use of the internet. Online Safety objectives are embedded throughout the computing curriculum and the PSHE curriculum. In Key Stage 2, 'Digital Leaders' are also trained in the key aspects of online safety with the aim of them helping to support other pupils and also parents at scheduled events.

The KCSIE 2025 section 'Online safety-advice' lists a number of resources for schools, parents and children which have been used by school staff to inform planning and Online Safety including communication with parents.

Cyberbullying

Cyberbullying is referenced in the Multi-Academy Trust's Anti-Bullying Policy though a more detailed explanation is offered here. The National Children's Bureau (2016) defines cyberbullying as: 'any form of bullying that is carried out through the use of electronic media devices, such as computers, laptops, smartphones, tablets, or gaming consoles', and adds that an instance of this would be 'an aggressive, intentional act carried out by a group or individual, using mobile phones or the internet, repeatedly and over time against a victim who cannot easily defend him or herself'.

This policy recognises the following as examples of cyberbullying though the list is not exhaustive:

• Bullying by text, calls, video, email or through social media on any device capable of sending communications.

• The use of technology to cause distress, fear or humiliation.

• Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social media sites and apps.

• Using digital devices to message others inappropriately.

• Hacking online accounts and/or creating fake accounts.

• Making threatening, abusive, defamatory or humiliating remarks in chat rooms and through social media sites and apps.

• Impersonating others on social media sites and apps by creating fake profiles or hijacking accounts.

Caedmon Primary School embraces the advantages of modern technology in terms of the educational benefits it brings. However, the school is mindful of the potential for bullying to occur. Central to the school's anti-bullying policy is the belief that 'all pupils have a right not to be bullied' and that 'bullying is always unacceptable'. The school also recognises that it must take note of bullying perpetrated outside school which has an impact on children in school.

Cyberbullying is generally criminal in character. The law applies to cyberspace as outlined below:

• It is unlawful to disseminate defamatory information in any media including internet sites.

• Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.

• The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

Caedmon Primary School educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through the PSHE and computing curriculums and assemblies, continue to inform and educate its pupils in these fast-changing areas.

Caedmon Primary School trains its staff to respond effectively to reports of cyberbullying or harassment and has systems in place to respond to it. We endeavour to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems. No pupil is allowed to work on the internet in the computer suites, or any other location within the school - which may from time to time be used for such work - without a member of staff present.

Whilst education and guidance remain at the heart of what we do, Caedmon Primary School reserves the right to take action against those who take part in cyberbullying. All bullying is damaging but cyberbullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts. Whale Hill Primary School supports victims and, when necessary, will work with the police to detect those involved in criminal acts. Caedmon Primary School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, either inside or outside of school.

Caedmon Primary School will use its power of confiscation, to include internet and learning platform access, where necessary to prevent pupils from committing crimes or misusing equipment. All members of the school community are aware they have a duty to bring to the attention of the Headteacher any example of cyberbullying or harassment that they know about or suspect.

Dealing with exposure to inappropriate materials: content, contact and conduct

Guidance to staff

If you suspect or are told about a content, contact or conduct, including cyber-bullying, incident, follow the protocol outlined below:

Mobile Phones

• Ask the pupil to show you the mobile phone.

• Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.

• Make a transcript of a spoken message, again record date, times and names.

• Tell the pupil to save the message/image (if appropriate).

• Go with the pupil and see the Head teacher, or in her absence, a member of the Senior Leadership Team.

Computers

• Ask the pupil to get up on-screen the material in question (if this is not possible the child could tell you how to find it on the screen and the website they were working within).

• Ask the pupil to save the material (if appropriate).

• Print off the offending material as a record (cyberbullying).

• Make sure you have got all pages in the right order and that there are no omissions.

• Accompany the pupil, taking the offending material, to see the Head teacher.

• Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

Guidance for Pupils

• If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, a teacher or your headteacher.

• Do not answer abusive messages but log and report them.

• Do not delete anything until it has been shown to your teacher, parents/guardian or the headteacher (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).

• Do not share personal IT details.

• Never reply to abusive e-mails, messages or texts.

• Never reply to someone you do not know.

Guidance for Parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyberbullying:

• Parents can help by making sure their child understands the school's policy and, above all, how seriously Whale Hill Primary School takes incidents of cyber-bullying.

• Parents should also explain to their children legal issues relating to cyberbullying.

• If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.

• Parents should contact the Head teacher as soon as possible. A meeting can then be arranged, which may involve other relevant members of staff.

If any teacher, pupil or parent suspects that any of our children are at heightened risk of exposure to inappropriate use of the internet, they should inform the Designated Safeguarding Lead as a priority.

Safeguarding Against Radicalisation and Extremism

At Caedmon Primary School, we consider protecting children against radicalisation and extremism is part of the school's wider safeguarding duties and is similar in nature to protecting children from grooming. This can include other risks such as drugs, gangs, neglect and sexual exploitation. We also acknowledge that some children may be vulnerable to radicalisation and, to fulfil our Prevent Duty, we ensure that staff are able to identify such children. We have a vital role to play in protecting our pupils from the risk of extremism and radicalisation. Keeping children safe from the risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other form of online abuse.

At Caedmon Primary School, if there are concerns over a child's safety at risk of radicalisation, Caedmon Primary School, will adhere to the following:

• In the first instance, our schools safeguarding policy will be adhered to.

• The local police lead for anti-terrorism will be informed.

• If the threat is imminent, and there is a concern that a child's life is in immediate danger, or that they may be planning to travel to Syria or Iraq, the risk is heightened and therefore an emergency call must be made – 999 or 0800789321 (Anti-Terrorist Hotline).

• Following a concern with regards to radicalisation and extremism the local authority or police might suggest a referral to the 'Channel' programme, which is a voluntary government funded programme which aims to safeguard children and adults from being drawn into terrorist activity.

More detail is provided in the school's Safeguarding Against Radicalisation and Extremism policy

Online Safety at home

In line with the school's approach to all aspects of safeguarding, parental engagement is considered essential in ensuring children are safe online. The school believes that parents are their children's first and best teachers and that they need to be equipped with the

knowledge and skills to support their children at home. In addition, more detailed half-termly resources are provided, and other carefully selected resources throughout the school year.

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Some examples of important and useful information that the school has shared with parents can be found on the following sites:

- www.thinkuknow.co.uk/
- https://www.commonsensemedia.org/
- www.saferinternet.org.uk
- www.net-aware.org.uk
- www.parentzone.org.uk
- http://vodafonedigitalparenting.co.uk/
- www.internetmatters.org

Managing Online Safety in School

There are a number of documents adhered to within school which audit the effectiveness of Online Safety within Caedmon Primary School:

Online Safety Policy – audited annually by all members of staff.

Child Protection & Safeguarding Policy – audited annually by all members of staff. Contains extensive references to Online Safety and its importance in the context of our school.

Acceptable Use Policy – audited annually by all members of staff.

Staff Behaviour Policy – updated with any new members throughout the year.

Home-School Agreement– signed by parents, children and teachers to ensure the standards and expectations of the school are upheld by all parties.

Accidental Access to Inappropriate Materials – updated as and when necessary.

Website Unblocking – updated as and when necessary, once the OneIT helpdesk has been notified.

Use of Personal Digital Devices within School – A document to log staff using their own devices either within school or on trips. Devices to be checked by John Frost or a member of SLT afterwards to ensure any images of the children have been removed.

Filtering and Monitoring Log– All Online Safety and unacceptable uses of the internet including social networking sites are to be logged in here. This log is then monitored by the head teacher termly.

Form of Consent for Use by the School and media of Photographs of Children – A document that must be signed by parents and carers for permission to use photographs and videos of children on the school website or social media. Without consent, images may not be used for these purposes. Consent is obtained in each key stage but can be withdrawn at any time.

Further information regarding Acceptable Use Policies and Digital Images can be found within the School's Acceptable Use Policy outlined in the Computing Policy.

<u>Use of technology for online / virtual teaching</u>

The Safer Recruitment Consortium (2020) issued an update relating to the increase in virtual teaching due to school closures during the Covid-19 outbreak. In the case of such an event, and any future event which may require the use of virtual teaching, guidance for staff is outlined below:

All settings should review their online safety and acceptable use policies and amend these if necessary, ensuring that all staff involved in virtual teaching or the use of technology to contact pupils are briefed on best practice and any temporary changes to policy / procedures. When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security.

Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled. In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc.

Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

The following points should be considered:

• think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred

• staff and pupils should be in living / communal areas – no bedrooms • staff and pupils should be fully dressed

• filters at a child's home may be set at a threshold which is different to the school

• resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content.

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

For home learning, Caedmon used ParentMail during the first Covid-19 Lockdown before moving to Seesaw due to its interactive design and features. These offer secure and reliable contact with parents. When sending home learning resources and contacting parents, staff devices have been used either in school or securely connected to the school network from home. Tasks sent directly to parents and children through Seesaw with instructions were initially favoured over virtual lessons so that parents are able to support children academically as well as help them to use online resources safely and responsibly. After reviewing the effectiveness of home learning during the second Covid-19 Lockdown, some activities were supplemented with live teaching and whole-year group assembly sessions. These were received positively by children and parents. More details are included in the school's Remote Learning Policy.

When telephone contact has been made with parents, it has been strongly encouraged that this be done in school and using the school's telephone. Staff who have chosen to telephone parents from home, it has been made clear that personal details be withheld using the phone's settings or by dialling with the prefix '141'

Acknowledgements:

Keeping children safe in education: Statutory guidance for schools and colleges. (2025) Department for Education. https://assets.publishing.service.gov.uk/media/686b94eefe1a249e937cbd2d/Keeping_children_safe_in_educatio n_2025.pdf [Accessed 25 July 2025]

Working Together to Safeguard Children 2023: A guide to multi-agency working to help, protect and promote the welfare of children (2023) HM Government. https://assets.publishing.service.gov.uk/media/669e7501ab418ab055592a7b/Working_together_to_safeguard_c hildren_2023.pdf [Accessed 25 July 2025]

Generative AI: product safety expectations. (2025) Department for Education. https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-productsafety-expectations [Accessed 27 July 2025]

Teaching online safety in schools: Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. (2023) Department for Education.

https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-inschools [Accessed 27 July 2025]

Meeting digital and technology standards in schools and colleges. (2025) Department for Education. https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/updates [Accessed 25 July 2025]

Revised Prevent duty guidance: for England and Wales. (2023) Home Office. https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-forengland-and-wales [Accessed 27 July 2025]

Guidance for safer working practice for those working with children and young people in education settings:

COVID addendum April 2020. (2020) Safer Recruitment Consortium. https://c-cluster110.uploads.documents.cimpress.io/v1/uploads/5aba001d-e2e6-42ee-b9cbbd44831f65f0~110/original?tenant=vbu-digital [Accessed 25 July 2025]

Focus on: Cyberbullying. (2016) National Children's Bureau https://antibullyingalliance.org.uk/sites/default/files/uploads/attachments/Focus%20on%20Cyberbullying-1_1.pdf [Accessed 25 July 2025]