CAVERSHAM PRIMARY SCHOOL

Caversham Primary School

Online Safety Policy

Reviewed November 2025

To be reviewed November 2026

The latest version of this policy is available on the school website and upon request.

Governors have had oversight of this policy and review and approve it annually.

Contents

1. Introduction

Caversham Primary School is committed to a whole-school approach to online safety and safeguarding that protects and educates students and staff in their technology use. We aim to ensure the online safety of pupils, staff, volunteers, and governors. We use training, education, and effective procedures to educate, empower and protect the whole school community when they are online. We recognise that the use of technology has become a significant component of many safeguarding issues, including child-on-child abuse. We take any concerns seriously and escalate these where appropriate.

In line with Keeping Children Safe in Education, we aim to address the following four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

The Designated Safeguarding Leads (DSLs) take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. The DSL's liaise with staff including the Computing Leader on matters of safety, safeguarding and welfare, including online and digital safety and when deciding upon a referral to relevant agencies.

We strive to consistently create a culture that incorporates the principles of online safety across all elements of school life. This helps to support our safeguarding culture.

The purpose of this policy is to ensure the safety and wellbeing of children when online and provide our staff and volunteers with the guidance and means to do this.

Our mechanisms to identify online safety concerns include our filtering and monitoring system, the direct work we conduct with pupils through our curriculum, and the training we provide to staff.

Where online safety concerns arise we utilise our Safeguarding Policy, Acceptable Use Agreements and Behaviour Policy if necessary to ensure an appropriate response. This could include but is not limited to:

- intervention work with pupils on online safety,
- adjustments to the curriculum to teach key ideas or strategies for staying safe online,
- the use of the Behaviour Policy,

Where necessary, we may need to escalate concerns around online safety. The Designated Lead would take a part in this decision-making process and where necessary external agencies would be involved.

2. Roles and responsibilities

2.1 The governing body:

- Take overall responsibility for this policy and its implementation
- Read, and understand this policy
- Ensure the policy is reviewed and updated annually
- Ensure students are taught about online safety
- Ensure staff and governors receive safeguarding training that includes online safety at induction, and that this is regularly updated
- Ensure online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures
- Ensure there are appropriate filtering and monitoring systems in place and regularly review the effectiveness of these systems

2.2. Co-Headteachers:

- Ensure staff understand this policy
- Ensure the implementation of this policy is consistent across the school
- Ensure any new members of staff learn about our approach to online safety at induction and regularly thereafter
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns

2.3 Computing Leader:

- Oversees the annual review of the school's approach to online safety, supported by the annual risk assessment that considers and reflects the risks that children face online.
- Takes the lead responsibility for online safety as part of their duties as deputy designated safeguarding lead
- Works with class teachers to address any online safety concerns or incidents, in line with our child protection and safeguarding policy
- Liaises with external safeguarding partners as necessary, including children's social care and the police and makes referrals with the support of relevant colleagues and their expertise
- Ensures any online safety incidents are recorded appropriately and that staff are aware of how to record online incidents
- Delivers staff training on online safety
- Provides regular updates regarding online safety incidents to the co- headteachers
- Understand the filtering and monitoring systems in place, manage them effectively and understand how to escalate concerns
- Ensures that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

2.4 Network/ICT Management Company (Soft Egg)

- Ensure appropriate filtering and monitoring systems are put in place
- Regularly review the filtering and monitoring systems to ensure students are safe from harm online
- Ensure that the school's ICT systems are secure and protected against viruses and malware
- Ensure that the school has an appropriate level of security protection and that this is reviewed periodically to keep up with evolving cyber-crime technologies.
- Ensure that the filtering and monitoring system flags safeguarding concerns to the DSL/ safeguarding team and regular reports are received

2.5 All staff and volunteers

- Read and understand this policy
- Assist with the consistent implementation of this policy
- Agree with and follow our acceptable use of IT agreement
- Agree with and follow the Staff Code of Conduct which outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.
- Refer any online safety safeguarding concerns to the DSL's or a Deputy DSL by email.
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, maintaining an attitude of 'it could happen here' and not dismissing any reports.
- Update parents around what their children are being asked to do online, including the sites they may be asked to access and who, if anyone, their child should be interacting with from the school online.

2.6 Parents

- Understand the importance of children being safe online
- Read, understand and comply with this policy
- Read the information shared with parents regarding acceptable use, what the school asks the child to be doing online, including the sites they will be asked to access and who from the school (if anyone) will be interacting with their child
- Notify a member of staff regarding any questions regarding this policy and its implementation
- Ensure their child has read, understood and agreed to the acceptable use of IT agreement
- Support their child to behave safely and appropriately online

3. Teaching online safety

In line with 'Teaching online safety in school,' published by the Department for Education in January 2023, we teach pupils about online safety and harms. Our teaching covers the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. These skills are covered in Computing, PSHE and RSE lessons, as well as regular assemblies.

Throughout this, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives, including:

- how to evaluate what they see online
- the risks posed by social media platforms
- how to recognise techniques used for persuasion
- unacceptable online behaviour
- how to identify online risks
- how and when to seek support
- how elements of online activity could adversely affect a pupil's personal safety or the personal safety of others online
- how elements of online activity can adversely affect a pupil's wellbeing

Pupils with SEND

We recognise that there are some pupils, for example those with special educational needs, who may be more susceptible to online harm. Such groups may also face additional risks, for example from bullying, grooming and radicalisation. We tailor our curriculum to meet the needs of these pupils by appropriate adjustments being made to teaching and learning. We will ensure these pupils receive the information and support they need through additional support and effective scaffolding.

In addition, our school completes an annual risk assessment for online safety. We consider the updated non-statutory guidance (Jan 2023) from the DfE on teaching online safety and how we teach these elements.

4. Filtering and monitoring

Caversham Primary School uses Securly as a filtering and monitoring system. This filters and monitors for acceptable use of the internet, blocking all forms of social media and inappropriate content. This covers our school network and the following devices: desktop computers, laptops, and iPads.

The Computing Leader has lead responsibility for understanding the filtering and monitoring systems and processes in place. The Computing Leader and DSLs monitor the effectiveness of this system through an annual review of the filtering and monitoring provision. The Computing Leader is supported by a governor in executing this duty. The governor is Professor Chris Guy and has a responsibility for cyber security.

The school takes care to not 'over block; content so that there are not unreasonable restrictions on what students can be taught regarding online safety.

The processes we have in place have been informed by our risk assessment as required by the Prevent Duty.

The DfE has published filtering and monitoring standards which set out that schools 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 reasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

We at Caversham Primary School have done the following in relation to this: our Computing Leader maintains an overview of our filtering and monitoring activity by conducting weekly checks on each of our filtering policies; in addition, out Computing Leader reviews the filtering and monitoring provision annually in conjunction with Soft Egg; and, as a school, we take actions to ensure that certain educational websites are unblocked in order to safely enrich our pupils' learning.

When the filtering and monitoring system detects concerning usage, we will record this on our safeguarding reporting system, CPOMS, and take appropriate action, including a referral to children's social care when necessary.

For more information on filtering and monitoring, parents and carers can contact the school office.

5. Security

Caversham Primary School has appropriate levels of security protection, and this is reviewed periodically to keep up with evolving cyber-crime technologies. This includes robust anti-virus and anti-spam software across our school network, individual password-protected pupil accounts for accessing our school laptops, and notifications of any offensive or concerning searches through our filtering and monitoring provider.

We have implemented the following technical measures to protect against cyber-crime:

(i) firewalls;

(ii) anti-virus software;

(iii) anti-spam software;

(iv) auto or real-time updates on our systems and applications;

(v) URL filtering;

(vi) secure data backup;

(vii) encryption;

(viii) deleting or disabling unused/unnecessary user accounts;

(ix) deleting or disabling unused/unnecessary software;

(x) using strong passwords; and

(xi) disabling auto-run features.

6. Educating parents about online safety

We recognise that parents can play a significant role in keeping their children safe online. To raise parents' awareness of online safety, we include online safety updates regularly in our weekly parent newsletter.

7. Acceptable use agreement

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. For further information on acceptable use please refer to the separate agreements below which detail our policy on personally owned devices, their use on premises and what is acceptable.

Any breaches of this agreement can lead to appropriate disciplinary action in line with our school's behaviour policy.

8. Use of mobile and smart technology

We recognise that 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, can sexually harass, abuse, bully or control their peers 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. To manage this and reduce risk, we only allow pupils in Years 5 and 6 to bring mobile phones into school and they not permitted to use them during the school day, or during morning or after-school clubs. Mobile phones must be handed in to a member of SLT at the school gates at the beginning of the school day, where they will then be held in the school office until the end of the school day.

Our Staff Code of Conduct outlines what we expect from staff in relation to use of mobile and smart technology, social media, and acceptable online communication with students.

In summary, in relation to tablets, game, consoles, mobile phones and wearable technology we outline the following for each group:

Staff

- Staff are allowed the use of mobile phones only when pupils are not present
- Staff are permitted to bring in wearable technology, such as smart watches, at their own discretion
- All personal tablets, games, and consoles are prohibited.

Pupils

- Pupils are only allowed to bring mobile phones into school in Years 5 and 6, and these must be given to a member of SLT at the beginning of the day, where they will be safely stored until the end of the day.
- Pupils are only allowed to bring in fitness trackers. All smart watches with camera and other features are prohibited.
- All personal tablets, games, and consoles are prohibited.

Parents

- Parents are prohibited from the use of mobile phones and any other devices on the school grounds.

In terms of the appropriate use of social media, we outline the following for each group:

Staff

- Staff are prohibited from using social media websites in school and this is a specific area of focus within our filtering and monitoring.

- Staff are encouraged to consider their digital footprint with regards to their recreational social media use and their associated behaviour.

Pupils

- Pupils are prohibited from using social media websites in school and this is a specific area of focus within our filtering and monitoring.
- As a school, we regularly speak to the pupils and educate them on the guidance around and the risks of using social media, including raising awareness of age limits.

Parents

- Parents are regularly reminded to refrain from sharing any photographs taken during school events on social media.
- Parents are regularly reminded of the risks of social media for young people and the age limits of the different social media websites and apps.
- Parents are advised to be vigilant with regards to their children's mobile phone and internet activity at home, including their behaviour on any groups on messaging apps.

9. Training and staff knowledge

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. This will also include training on the filtering and monitoring system used by the school and an understanding of expectations, applicable roles and responsibilities in relation to this.

All staff members will receive refresher training at least annually as part of our safeguarding training programme, as well as regular updates where relevant (for example through emails, e-bulletins and staff meetings).

The DSLs and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually. This will equip staff with the relevant knowledge and skills to safeguard children effectively, including online.

All staff should be aware and know:

- The indicators of abuse and neglect understanding that children can be at risk of harm inside and outside of the school/college, inside and outside of the home and online.
- To take reports of online harmful behaviour seriously and report them according to the school procedures.
- 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.
- That children can abuse other children online, this can take the form of:
    - Online abuse, including sexual
    - Online harassment, including sexual
    - Cyberbullying
    - Misogynistic/ misandrist messages,
    - the non-consensual sharing of incident images, especially around chat groups,

- and the sharing of abusive images and pornography to those who do not want to receive such content.
- That child-on-child abuse could be happening in the school setting and that this could be taking place online. All incidents of child-on-child abuse should be reported in line with our reporting systems.

More information about safeguarding training is set out in our child protection and safeguarding policy.

10. Anti-Bullying and child-on-child abuse

We recognise that our approach to online safety should strengthen the work we do around anti-bullying. As a Rights Respecting School, the anti-bullying approach of the school is consistent with the UN Convention on the rights of the child. All staff and pupils promote values that reject bullying behaviour and promote co-operative behaviour. We teach our pupils that bullying is unacceptable and we respond to reported acts of bullying promptly and effectively.

Our work on online safety helps to tackle bullying by regularly reminding pupils of the different forms of bullying, including cyber bullying, and of the importance of pro-social behaviour online. Pupils are reminded of the avenues available if someone is unkind to them online and they are encouraged to treat others with empathy at all times.

In addition, we understand that online behaviour can also constitute child-on-child abuse. We respond to incidents of child-on-child abuse in line with our Safeguarding Policy and Behaviour Policy, this includes reporting the incident on CPOMS and informing both sets of parents of the incident and the associated consequences for the pupil(s).

11. Further information to support you

We work with our local safeguarding partners to ensure our students are safeguarded. We will liaise with these partners where there are safeguarding concerns and will follow their policies and procedures when needing their support. This may include referrals or seeking advice from Children's Social Care, our local Prevent team and/ or the police.

For **parents** the following websites could be of use:

- Samaritans: Talking to your child about self-harm and suicide content online
- NSPCC Online Safety Guides for parents
- Report harmful content at https://reportharmfulcontent.com/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/
- CEOP - how to help your children get the most out of the internet
- Further guidance shared by the DfE can be accessed here

For **students** the following websites could be of use:

- Mind- mental health support
- Togetherall- online community accessible 24/7
- Shout- a free text service available 24 hours a day. You can start a conversation by texting Shout to 85258
- Samaritans' self-help app
- Kooth is an online mental wellbeing community for young person
- Report harmful content at https://reportharmfulcontent.com/child/
- Report concerns to the NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-reporting/

For **all staff and volunteers** it is useful to be aware of the resources available to staff and students so that you can signpost them as required. In addition, the following resources could be of use:

- UK Safer Internet Centre- practical resources, advice, and training to support safe and responsible internet use.
- internetmatters.org – research, free lesson plans, and resources to support the teaching of online safety and digital literacy across subject areas.
- DfE guidance Teaching online safety in schools - non-statutory guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Policies/ guidance to be read and understood alongside our online safety policy:

- Safeguarding/ Child Protection policy.
- Behaviour policy.
- Staff Code of Conduct inc. acceptable use of technology in the staff behaviour policy/ code of conduct.
- Anti-bullying procedures including cyberbullying

- The Prevent Duty and The Prevent duty: an introduction for those with safeguarding responsibilities
- Meeting digital and technology in schools and colleges (DfE)

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will hand it in to a member of SLT on the school gate at the start of the day, where it will be safely stored until the end of the school day. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**