



Leeds East
Primary Partnership
A CO-OPERATIVE TRUST

Cross Gates
Primary School

Policy and Procedure

Cross Gates Primary School

Online Safety Policy

Written by: Sophie Wilkinson

Ratified by Governors: Oct 2018

Reviewed: Nov 2020

Reviewed: Jan 2023

Reviewed: March 2024

Reviewed: September 2025

Reviewed: September 2026

Review Date: September 2027

Legislation and guidance

This policy is based on the statutory safeguarding guidance, [Keeping Children Safe in Education](#) from the Department for Education (DfE) and its advice for schools on:

- [Teaching online safety](#)
- [Meeting digital and technology standards](#)
- [Preventing and tackling bullying](#)
- [Relationship and Sex Education \(RSE\) and Health Education](#)
- [Searching, screening and confiscation](#)
- [Mobile phones in schools](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), the [Children's Wellbeing and Schools Act 2026](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study. This school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff and volunteers to share this commitment.

Aims

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- To identify and support groups of pupils that are potentially at greater risk of harm online than others
- To deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- To establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- To provide staff and volunteers with the overarching principles that guide our approach to online safety
- To ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices
- To value skills and contributions of pupils, staff and the wider school community using and integrating useful ideas.
- To ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- To educate pupils, staff and the wider school community in their use of technology
- The online safety policy is integrated with other relevant policies
- Online safety will be taught across the school curriculum

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Cross Gates Primary School's activities.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Cross Gates' network and devices

- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety

Understanding the Risks

Areas for online risks can be categorised into the 4 C's - Content, Contact, Conduct and Commerce, and can be commercial, aggressive or sexual in nature as shown in the table below.

We understand that online risks arise when a child:

- engages with and/or is exposed to potentially harmful **CONTENT**;
- experiences and/or is targeted by potentially harmful **CONTACT**;
- witnesses, participates in and/or is a victim of potentially harmful **CONDUCT**;
- is party to and/or exploited by a potentially harmful **COMMERCE**.

4 C's	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Commerce Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity eg trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualisation of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate use-generated or marketing content, mis/disinformation	Ideological persuasion, radicalisation and extremist recruitment	Potentially harmful use communities eg elf-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

We will seek to keep children and young people safe by:

- appointing an online safety coordinator – Sophie Wilkinson (Headteacher/Designated Safeguarding Lead)
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers

- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- implementing a system whereby pupils always use the same devices in lessons so that any searches which may indicate a child is at risk can be traced back to the correct child and action can be taken
- using Smoothwall as our firewall software which blocks inappropriate content and notifies the Headteacher who has made the search so that action can be taken if necessary. Smoothwall is a DfE accredited filter provider with the UK Safer Internet Centre (UK SIC). *Fundamentally web filters and firewalls serve **different purposes**. A web filter blocks access to specific types of web content and a firewall prevents your network from exposing internal services and computers to external threats. Traditional firewalls and web filters operate at different layers of the Open System Interconnection (OSI) model*
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been give
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and Child Protection Policy
- Keeping Children Safe in Education
- Safer Working Practice
- Use of Mobile Phones Policy
- AI Policy
- Searching and Confiscation Policy
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Positive Behaviour Management
- Data Protection and GDPR
- Photography and image sharing guidance. The NSPCC information (updated 9 July 2026) can be found here <https://learning.nspcc.org.uk/online-safety/photographing-filming-children> LCC guidance for Staff working in Educational Settings on the Use of Digital

Roles and Responsibilities

Governors

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

The governor who oversees online safety is Karen Jessup.

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances. All designated staff have full access to CPOMS and access to the safeguarding email address to make sure safeguarding concerns are received, monitored and acted on without delay.

The Headteacher will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Headteacher will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Headteacher will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Headteacher will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The board will review the [DfE's filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

- Staff are given appropriate training and are made aware that all internet activity within school is monitored.
- Staff are given time to update skills and learn to integrate new applications within their teaching.
- Fully conversant with the online safety policy and rules of internet access and reporting procedures.
- Routinely teaching online safety across the curriculum.
- Activity reports are monitored regularly and action taken as necessary.
- Parents' attention will be drawn to the policy through Reach More Parents (weduc) and the website.
- An online safety scheme of work is incorporated within each year group's curriculum, covering both school and home use.
- The policy is regularly reviewed and correctly implemented.

DSL

Details of the school's designated safeguarding lead (DSL), deputy and safeguarding officers are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT technician and business manager to make sure the appropriate systems and processes are in place
- Working with the deputy headteacher and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the DSL.
- Working with the DSL to make sure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Ensuring online safety is taught as part of the whole school curriculum and referred to within every online access session.
- Rules for online access and email use are posted near computer systems and discussed within classrooms.
- They supervise pupils when they access the Internet, no child is unsupervised when accessing online material.
- They use the Internet in a responsible manner, in line with Leeds City Council guidance.

This list is not intended to be exhaustive.

Pupils

Pupils should ensure;

- Through the computing curriculum, they read and follow the Rules for Responsible use guidance or have them explained by a teacher where necessary
- They access the Internet in a sensible manner.
- They report to an adult if they intentionally or unintentionally access any inappropriate or offensive material.
- They refrain from giving their name, address or contact numbers to any person without permission from a parent, carer or teacher.
- Mobile phones are only permitted to be brought into school in Year 5 & 6 and should be switched off as soon as children enter school grounds and not switched on until they have left school grounds at the end of the day. They should be handed in to the class teacher as they enter the classroom and returned when they leave. Children are not permitted to enable WIFI nor 4G connectivity through personal devices during school time. This applies also to extra-curricular activities and when children are on school related trips (eg, residential).

This list is not intended to be exhaustive.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Parents and carers are encouraged to reinforce and discuss this policy at home as appropriate, including the risks associated with mobile phone use and the benefits of a mobile phone-free environment.

Cross Gates Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records

Due to the increased use of the Internet in the home, so much more can be achieved if parents and guardians are involved in their child's education and understanding. As such, Cross Gates Primary has;

- Photo-consent letters to be sent home when any child joins school
- Regular letters and relevant leaflets and information will be sent home with your child or through the free Reach More Parents app
- An online safety section will be included in the weekly newsletter
- Posts of current news and information will be posted on RMP
- All parents/guardians/children will have access to the school website and links for e-safety and safe sites for all will be provided to parents
- Email access to all parents via admin@crossgatesprimary.co.uk

Parents/carers are asked:

- Not to take pictures or recordings of pupils, unless it is at a public event or it is their own child
- To use photographs/recordings for personal use only and not to post on social media

Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

Pupils using mobile devices in school

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the headteacher.

Cyberbullying

In line with the anti-bullying policy and the positive behaviour management policy, cyberbullying will be dealt with in the following way:

- Complaints are taken seriously and dealt with quickly
- The senior leadership team will investigate the complaint
- Parents will be informed
- Incidents of bullying are recorded and kept on record
- This is monitored to see if there are any patterns arising
- Close monitoring and supervision, particularly on the playground
- Children who bully will be dealt with following the school's behaviour management policy
- Both the victim and the bully will be made aware of the action taken
- Persistent bullies will be closely monitored and supervised

- If appropriate, the victim and the bully will receive counselling and/or support
- If appropriate, outside agencies will be involved, usually for persistent bullies
- Sometimes, victims of bullying may provoke other children. This does not excuse the bullying, but we help the victim to understand that their behaviour may be contributing to the problem
- We try our best to ensure the victim has friends s/he can rely on

Educating pupils about online safety

Teaching and Learning

Internet access will be planned to enrich and extend learning activities. Pupils will be given clear objectives for Internet use. We have a progressive curriculum that is flexible, relevant and engages pupils' interest; it must be used to promote online safety through teaching pupils how to stay safe, to protect themselves and others.

Curriculum mapping, within ICT, ensures that coverage is structured to build upon previous learning avoiding needless repetition.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure

Relevant safety information can be supported through THINKUKNOW and CEOPS materials and interactive activities. Staff might also refer to: <http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/> <http://www.theschoolrun.com/how-keep-your-child-safe-online> <http://www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx> (KS2)

Where there are children with SEND, provision should be adapted to suit their capabilities.

All teaching will be widened to incorporate Internet content issues, for instance the value and credibility of Web materials in relationship to other media, such as books and newspapers.

Rules for Responsible Use:

Our Internet Rules:

- We ask permission before using the Internet
- We use web-sites our teachers have advised us to look at
- We only e-mail/message people our teachers have asked us to

- When we send e-mails/messages they are polite and friendly
- We never give out our address or telephone numbers
- We never arrange to meet anyone we don't know
- We don't open e-mails/messages from people we don't know
- We tell a teacher if we see anything that we are unhappy with

How should we act on the Internet?

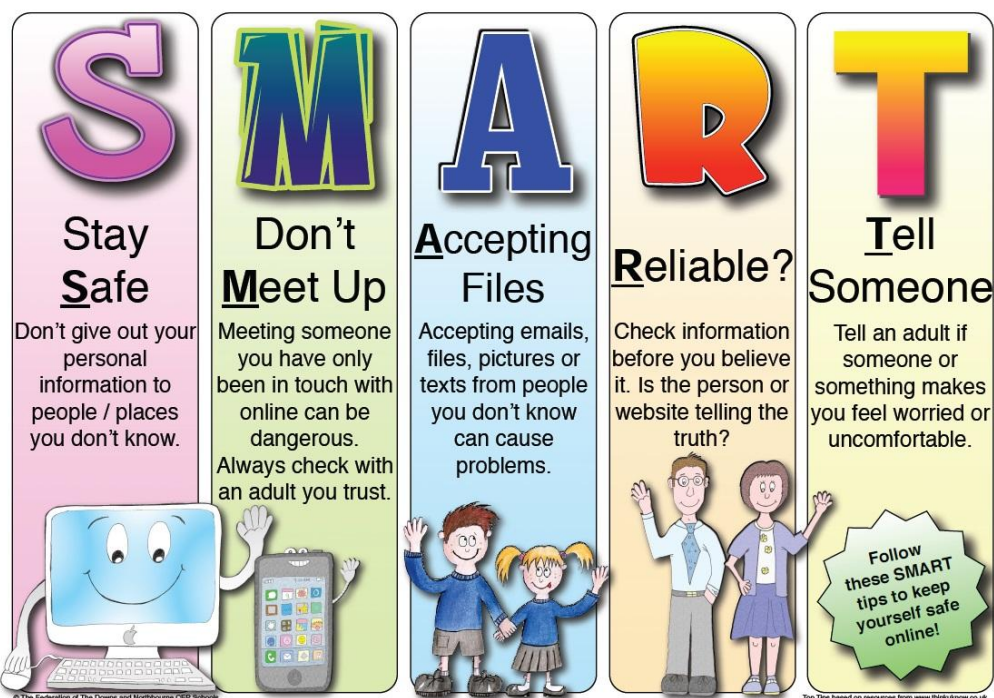
S Keep your personal information **SAFE** and **SECURE**

M Do not agree to **MEET** anyone from the Internet; they may not be who you think they are

A Do not **ACCEPT** messages or e-mails from somebody you don't know.

R **RELIABLE**, do not always trust the information you find on the Internet; it may not be correct

T If something or someone upsets you on the Internet **TELL** a trusted adult in school or at home



Acceptable Use of the Internet

- Access must only be made via the user's authorised school account and password, which must not be given to any other person.
- School computer and Internet use must be appropriate to the student's education or to staff professional activity. Any resources shown to or used by the children should be re-checked shortly before the children see it, so as to ensure appropriate content. This includes videos and activities alike.
- Copyright and intellectual property rights must be respected.
- Users are responsible for email they send and for contacts made.
- Email should be written carefully and politely. Messages should be written in the knowledge that they may be forwarded on/become relevant outside the context of the email or text. As such, when composing emails, due regard should be given to the professionalism of the content.
- Anonymous messages and chain letters must not be sent.
- The use of public chat rooms in school is not allowed.
- The school IT systems may not be used for personal purposes, unless the Headteacher has given permission for that use.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- The security of IT systems must not be compromised, whether owned by the school or by other organisations or individuals.
- Serious Internet abuse may result in the loss of Internet access or disciplinary action.

Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device in line with the school's searching and confiscation policy.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will not:

- View, copy, print, share, store, save, forward on, or ask a child to share or download, the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

The staff member will confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support. Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy/searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Cross Gates Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes' or 'deep nudes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Cross Gates Primary School will treat any use of AI to bully pupils very seriously, in line with our anti-bullying and positive behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI usage policy.

Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of [3 random words](#), in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher or ICT technician.

Staff use of personal devices

In line with Safer Working Practice Guidance:

- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode.
- Staff handheld devices, including mobile phones and personal cameras must not be used during lesson times. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families outside of the setting in a professional capacity unless on a school trip or unless permission has been given by the headteacher.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they

must hide their caller identification. They can do so by inputting 141 or via the phone's settings to hide their own mobile number for confidentiality purposes.

- Staff can use their personal phones to contact a member of SLT, the safeguarding team or the school office in the case of an emergency. They can also use their personal phones to call 999 in the case of an emergency.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose. The only circumstances in which a teacher can take a picture on the mobile phone is on a school trip and/or so that the image can be uploaded on the school's official twitter account. **It should only be done with prior consent from the Head teacher.** The image should be taken in the presence of a teacher. The image/images should be deleted immediately once it is downloaded from the device or uploaded onto the school's official twitter account.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Monitoring and filtering arrangements

Internet access is currently provided through ICT4Leeds which includes using Smoothwall filtering appropriate to the age of pupils. Children will access the Internet through their local area network username and password. Structured lessons will be given, within Y2, to introduce and teach children the importance of online security along with an introduction to blogging and email. These skills will be reinforced throughout KS2 when the children may have their own blog and email account.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly.
- Workshops and guidance will be offered to the wider community annually.
- The school website, which reflects the school's ethos, includes safe links. Information is accurate and well presented.
- Social networking and personal publishing. Posts on the school Twitter feed are monitored regularly and offensive material removed.

Website Management

- The Headteacher will delegate some editorial responsibility to administrative staff and class teachers are responsible for maintaining content on class pages. Staff must ensure that content is accurate and quality of presentation is maintained.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Copyright and plagiarism laws will be adhered to.
- The contact information given will be the school's address, telephone or email. No personal information will be published.
- Photographs will only be published if parental consent has been given. No child will be identified by full name.

www.crossgatesprimary.co.uk

Training

All staff completed the *Online Safety and the Links to Child Protection* training in 2026. Staff receive regular safeguarding training which includes online safety. Training is also delivered via staff meetings, briefing updates and guidance documents.

Remote Learning

Safeguarding, including online safety, while remote learning is in place.

While many children will be learning remotely at this time, the safeguarding principles do not change:

- The best interests of children must always come first.
- If anyone has a safeguarding concern, they should act immediately.
- A DSL or deputy is always available when children are in school or remote learning, and all staff know how to contact them.
- Unsuitable people must not be allowed access to the children.
- Children continue to be protected while they are remote learning.

All staff made aware of the main challenges and risks to children learning remotely at home:

- Child sexual abuse through an online virtual environment.
- Peer on peer online abuse.
- Youth produced sexual imagery.
- Mental health issues being caused or exacerbated by the anxiety of the situation, family issues, isolation from real-life social networks or online experiences.

All staff familiar with potential indicators and response to:

- Peer-on-peer online abuse.
- Cyber-bullying, coercion, sexting, radicalisation.
- Indecent images of children.
- Coercing vulnerable young people into sharing inappropriate content.
- Mental health concerns.

Safeguarding Remote Learning

- Records to be kept of risk assessments undertaken for live streaming or pre-recorded lesson videos.
- Staff informed of new/revised practices with clearly explained practical instructions and expectations.
- Remote learning platforms appropriate and allow SLT to monitor lessons.
- Staff are supported via phone or online for technical support.
- Staff are supported via phone or online by a trained DSL or deputy.
- Staff are supported via phone or online for mental well-being.
- Parents and children supported by welfare phone calls, with mental well-being as well as academic progress in mind. Staff, parents and pupils are signposted to various practical support and guidance available on online safety and how to report concerns.
- Guide parents to support their children in dealing with technology, digital media, online teaching and the associated risks.
- Safe practice reinforced with the children.
- Where staff are remotely accessing the school network, filtering and monitoring systems remain in place.
- Pupils and parents can authenticate who is connecting with them online.
- Staff maintain professional communications via remote learning.
- Live video lessons are never 1:1.
- Staff remain fully compliant with data protection regulations.

- Staff only use school email accounts, school devices (where possible) and approved education programmes, platforms and systems for remote learning that are Data Protection compliant.
- Staff ensure documents, sensitive school and pupil data are kept confidential and secure.
- Staff are to keep equipment, passwords and data encryption safe and secure.
- School equipment is to be used strictly for school teaching and related projects.
- Staff must refrain from downloading suspicious, unauthorized or illegal software.
- Any items on loan from school must be returned if requested.

Air Tags

The use of air tags is prohibited from trips and visits following the triggering of anti-stalking software on iPhones on trips, the lack of consent to track and the safeguarding issues that arise in revealing the exact locations of children who may have court orders, are looked after (fostered/in care) and those children that need to be protected from this tracking.

**If you do not agree to the terms and conditions in this policy,
you will not be allowed online access.**