Leeds East
Primary Partnership
A CO-OPERATIVE TRUST

Cross Gates
Primary School

Policy and Procedure
Cross Gates Primary School

Online Safety Policy

Written by: James Garden/Sophie Wilkinson

Ratified by Governors: Oct 2018

Reviewed: Nov 2020

Reviewed: Jan 2023

Reviewed: March 2024

Review Date: March 2025

Legislation and guidance

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse **learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse**
- bullying **learning.nspcc.org.uk/child-abuse-and-neglect/bullying**
- child protection **learning.nspcc.org.uk/child-protection-system**

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 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 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 educate pupils, staff and the wider school community in their use of technology.
- To have appropriate mechanisms to intervene and support any incident where appropriate.
- To teach the statutory curriculum.
- To value skills and contributions of pupils, staff and the wider school community using and integrating useful ideas.
- To have a clear set of rules and reporting procedures agreed by staff, governors and school council.
- 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 – James Garden (Head Teacher/Designated Safeguarding Officer)
- 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 head teacher 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
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- 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 11 January 2024) can be found here https://learning.nspcc.org.uk/online-safety/photographing-filming-children#:~:text=Gaining%20consent%20to%20take%2C%20use,taking%20a%20photo%20or%20video
- LCC guidance for Staff working in Educational Settings on the Use of Digital Technologies and Social Media ArtForms-Guidance-for-staff-working-in-educational-settings-on-the-use-of-digital-technologies-and-social-media.pdf (artformsleeds.co.uk)

Roles and Responsibilities

Governors should ensure;

- This Online document is shared with all staff and they have been given the opportunity to discuss the policy.
- The policy is ratified and reviewed.
- The policy is read in conjunction with other statutory safeguarding policies (KCSIE).

Headteacher should ensure;

- 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.
- Using secure storage devices to protect data of all pupils and staff.
- Activity reports are monitored regularly and action taken as necessary.
- Parents' attention will be drawn to the policy through ParentMail and the website.
- An online safety scheme of work is incorporated within each year group's curriculum, covering both school and home use.

- New facilities will be thoroughly tested before pupils are given access.
- The policy is regularly reviewed and correctly implemented.
- Online safety is promoted within assembly.
- Personal data of all pupils and staff is protected.

Staff should ensure;

- Rules for online access and email use are posted near computer systems and discussed within classrooms.
- Online safety is taught as part of the whole school curriculum and referred to within every online access session.
- There is equality of access within the classroom.
- They follow correct reporting procedures for any incident which may arise.
- 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.

Pupils should ensure;

- Through the Purple Mash 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 6 and should be handed in to the class teacher at the start of the day and returned again at the end of the day. 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, residentials).

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. 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;

- Home/School agreement and Photo-consent letters will 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 ParentMail app.
- Posts of current news and information will be posted on X @CGPrimarySchool
- 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@crossgates.leeds.sch.uk

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.
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)

In KS1, staff will select sites which support the learning outcomes planned for pupils. Approved sites can be bookmarked, listed or copied to the favourites section.

In KS2, staff will decreasingly select sites, to encourage independent and safe searching. Pupils will be educated in taking responsibility for Internet access; actively encouraged to make correct choices for themselves and others. Peer mentoring may be used to assist and reaffirm the skills to locate, retrieve and evaluate information accessed.

Where there are children with SEND, provision should be differentiated 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.

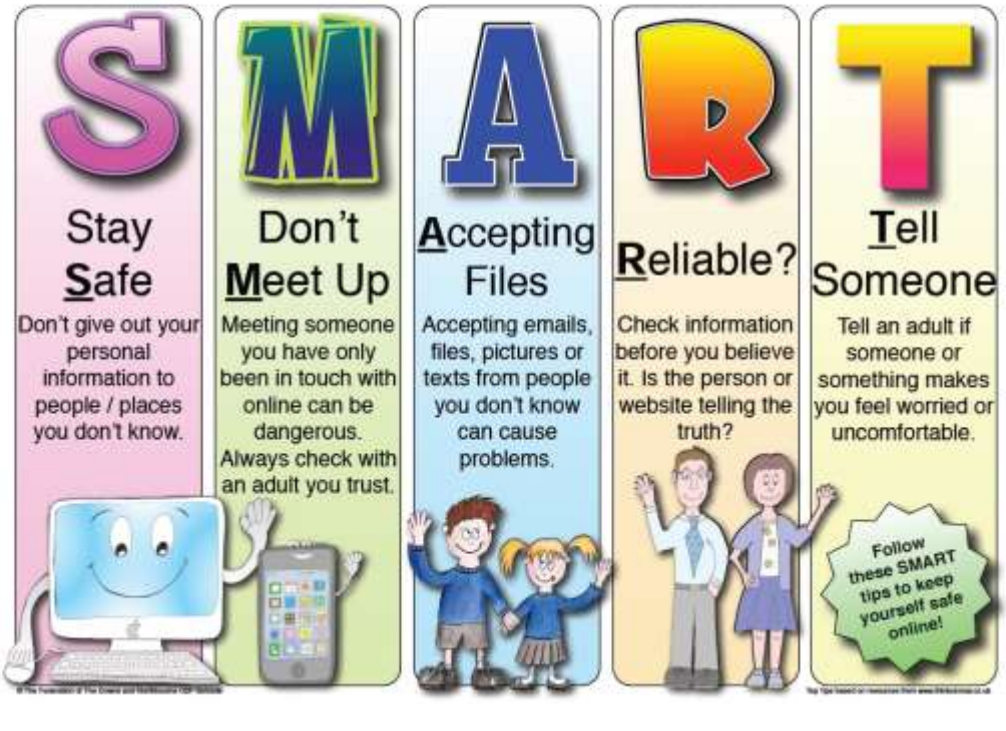
Rules for Responsible Use:

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 **S**AFE and SECURE
M Do not agree to **M**EET anyone from the Internet; they may not be who you think they are
A Do not **A**CCEPT messages or e-mails from somebody you don't know.
R **R**ELIABLE, 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 **T**ELL a trusted adult in school or at home


S
Stay Safe
Don't give out your personal information to people / places you don't know.
M
Don't Meet Up
Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.
A
Accepting Files
Accepting emails, files, pictures or texts from people you don't know can cause problems.
R
Reliable?
Check information before you believe it. Is the person or website telling the truth?
T
Tell Someone
Tell an adult if someone or something makes you feel worried or uncomfortable.
Follow these SMART tips to keep yourself safe online!

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.

Staff use of personal devices

In line with Safer Working Practice Guidance:

- 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.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode.
- 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.

- 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.

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.

Training

All staff completed the *Online Safety and the Links to Child Protection* training in 2022. 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.

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