St Chad's
Academies Trust

Mereside
Church of England Primary Academy
Learn to Love, Love to Learn

Online Safety Policy

Date of next policy review	June 2026
Name of person responsible for this policy	Lindsey Hughes & Kieran Bourke
Other related policies	Safeguarding Child Protection, Pastoral Care, Anti-Bullying Policy, SEN and T&L.
Issued to	Staff, Governors, Parents, Pupils
Date issued	

Children first: in the footsteps of St. Chad

As we follow Christ in the footsteps of St. Chad, we seek to be servant leaders who have a desire to see all those, within our Trust family, truly flourish both spiritually and academically

Contents

Key Principles / Vision

Our school aims to educate, empower, and protect pupils so that they develop safe, responsible, and respectful online behaviours. Online safety is an essential part of safeguarding, and we recognise that safeguarding incidents can occur both online and offline, inside or outside school.

1 Aims

Our school aims to ensure the online safety and wellbeing of all pupils, staff, volunteers, and governors. We aim to:

- Have robust processes in place to protect children and adults from online harm.
- Deliver an effective approach to online safety that empowers the whole school community to use technology safely, including mobile, smart, and emerging technologies such as Artificial Intelligence (AI).
- Establish clear mechanisms to identify, respond to, and escalate online safety concerns where appropriate.
- Embed online safety within our wider safeguarding culture, recognising that safeguarding incidents can occur both online and offline, inside or outside school.

2 Scope

This policy applies to all members of the school community and covers online activity:

- Using school-owned or personal devices.
- On school premises and off-site.
- During the school day, remote learning, or out-of-school hours where incidents impact pupils or staff.

3 Categories of Risk

Our approach to online safety addresses four key areas:

- **Content**: Exposure to illegal, inappropriate, or harmful material, including pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, and online sexual abuse.

- **Contact**: Harmful interactions with others online, including peer-to-peer pressure, inappropriate messaging, commercial advertising, adults posing as children to groom or exploit, and online sexual exploitation.

- **Conduct**: Personal online behaviour that increases the likelihood of harm, such as sharing images, cyber-bullying, or inappropriate communication.

Commerce: Risks including online gambling, inappropriate advertising, phishing, and financial scams.

Emerging and Evolving Risks

The school recognises that online risks continue to evolve. Current and emerging risks include:

- Exposure to harmful online influencers and content promoting misogyny or harmful ideologies
- “Sextortion” and coercion involving the sharing of images
- The use of artificial intelligence to create misleading, harmful, or manipulated content (including deepfakes)
- Risks linked to livestreaming, group chats, and private messaging apps
- Online gambling elements within games (e.g. loot boxes)
- Misinformation and disinformation

Staff receive regular updates to ensure they are aware of current risks and how these may present in school.

4 Legislation and Guidance

This policy is based on statutory guidance, including:

• Keeping Children Safe in Education (KCSIE, 2025)
• Teaching Online Safety in Schools
• Preventing and Tackling Bullying and Cyber-bullying
• Relationships and Sex Education (RSE)
• Searching, Screening and Confiscation
• Prevent Duty Guidance

Relevant legislation includes: Education Act 1996, Education and Inspections Act 2006, Education Act 2011, Equality Act 2010, Data Protection Act 2018, and UK GDPR. The policy also reflects the National Curriculum computing programmes of study.

5 Roles and Responsibilities

Governing Board

The governing board is responsible for:

- Monitoring this policy and holding the Headteacher to account for its implementation.
- Ensuring staff receive regular safeguarding and online safety training.
- Ensuring suitable filtering and monitoring systems are in place and reviewed at least annually.
- Ensuring online safety education is embedded across the curriculum.
- Ensuring safeguarding arrangements meet the needs of vulnerable pupils, including those with SEND.

Headteacher

The Headteacher is responsible for:

- Implementing this policy day-to-day.
- Ensuring all staff understand and consistently follow online safety procedures.

Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL)

The DSL takes lead responsibility for online safety with support from DDSL and will:

- Manage online safety concerns and incidents in line with safeguarding procedures.
- Ensure incidents are logged and responded to appropriately.
- Provide staff training and updates on online safety and emerging risks.
- Liaise with external agencies (e.g., police, LADO, children's services) when required.
- Conduct regular and ongoing risk assessments reflecting pupils' online experiences, informed by safeguarding logs, filtering and monitoring alerts, pupil voice, and local and national safeguarding trends.
- Report regularly to the Headteacher and governing board.

The DSL ensures that online safety is considered within all safeguarding decisions and that appropriate action is taken in line with the school's Child Protection and Safeguarding Policy.

Computing Lead

The Computing Lead is responsible for:

- Ensuring online safety and digital literacy are embedded across computing lessons, special events, and school projects.
- Liaising with the PSHE lead and other staff to ensure online safety and digital skills are reinforced across the curriculum.
- Supporting staff and volunteers with guidance on safe use of technology and emerging risks.
- Supporting the logging of online safety incidents and ensuring appropriate follow-up with the DSL and Headteacher.
- Supporting staff in addressing cyber-bullying incidents in line with the Behaviour Policy.
- Ensuring pupils are taught to use technology safely, responsibly, and respectfully, including age-appropriate guidance on AI.
- Keeping up to date with developments in computing education and online safety, sharing good practice, and helping embed digital skills across the school.

ICT Manager (externally sourced)

The ICT Manager is responsible for:

- Maintaining the security of the school's network, servers, and devices.
- Implementing and reviewing filtering and monitoring systems to prevent access to harmful content.
- Applying software updates, antivirus, and malware protection to school devices.
- Providing technical support and troubleshooting for network, hardware, and software issues.
- Supporting staff in secure handling of data and managing access rights.
- Escalating technical issues affecting online safety to the Headteacher or DSL.

All Staff and Volunteers

All staff and volunteers are expected to:

- Maintain professional boundaries at all times.
- Implement this policy consistently.
- Respond promptly to online safety concerns and report them to the DSL.
- Maintain an attitude of "it could happen here."

Parents and Carers

Parents and carers are expected to:

- Support the school in promoting safe and responsible online behaviour.
- Ensure their child understands and follows the school's acceptable use expectations.
- Raise concerns with the Headteacher or DSL.
- Access trusted guidance from organisations such as the UK Safer Internet Centre, Childnet, and Parent Info.

Visitors and Community Members

Visitors and community users are expected to:

- Be made aware of this policy where relevant.
- Follow the school's ICT and internet acceptable use guidance

6 Filtering and Monitoring Systems

The school uses appropriate filtering and monitoring systems to safeguard pupils when using technology. These systems are designed to:

- Prevent access to illegal, harmful, or inappropriate content
- Identify potential safeguarding concerns through monitoring of online activity
- Alert relevant staff to potential risks in a timely manner

Filtering systems block unsuitable content, while monitoring systems review user activity, including searches and online behaviour, to identify safeguarding risks.

Monitoring alerts are reviewed regularly by designated staff and are recorded, tracked and logged with actions taken through the school's safeguarding recording system.

Alerts are prioritised based on risk. Any alerts indicating potential safeguarding concerns (e.g. self-harm, sexual content, bullying, or radicalisation) are reviewed promptly and escalated immediately to the Designated Safeguarding Lead (DSL) where appropriate.

The school recognises that filtering does not remove all risk and that monitoring plays a key role in identifying concerns. Staff remain vigilant and do not rely solely on technical systems to safeguard pupils.

The school ensures that filtering and monitoring systems are:

- Age-appropriate and regularly reviewed
- Effective across all devices and networks used by pupils
- In line with DfE filtering and monitoring standards

The school works in partnership with its technical provider to ensure filtering and monitoring systems are appropriately configured, regularly reviewed, and effective in identifying safeguarding concerns.

The governing board receives regular updates on the effectiveness of these systems.

7 Educating Pupils About Online Safety

Online safety education is embedded across the curriculum through:

- Regular assemblies and themed events (e.g. Safer Internet Day).
- PSHE & RSE – following the Jigsaw scheme of work.
- Opportunities for pupil voice to influence online safety provision.
- Consistent reinforcement of online safety messages across the curriculum.
- Staff modelling safe and responsible use of technology.

Pupils are taught to:

- Use technology safely, responsibly, and respectfully.
- Keep personal information private.
- Recognise worrying or unsafe situations and know how to seek help.
- Understand that people may behave differently online than face-to-face.
- Evaluate online content and sources appropriately for their age.
- Recognise consent in online interactions and know how to respond safely.
- Understand how personal information and data are shared and used online.

Age-appropriate teaching:

- EYFS and KS1: Online safety education is adult-led; concerns may be identified through behaviour, play, or emotional responses.
- Additional support is provided for vulnerable pupils, including those with SEND, to ensure online safety teaching is accessible, adapted, and reinforced where needed.

8 Educating Parents About Online Safety

The school supports parents and carers through:

- Newsletters, letters and the school website (Wake Up Wednesdays).
- Workshops and information sessions.
- Signposting to trusted organisations such as UK Safer Internet Centre, Childnet, and Parent Info.

9 Cyber-Bullying

Definition: Repetitive, intentional harm of a person or group online.

Prevention and Response:

- Pupils are taught how to recognise and report cyber-bullying.
- Clear reporting routes are provided.
- Victims are supported, and behaviour is addressed in line with Behaviour and Safeguarding Policies.
- Sanctions are applied proportionately, alongside education and support.
- Staff may search and delete inappropriate content on pupils' devices in line with DfE guidance.

10 Youth-Produced Sexual Imagery

- Treated as a safeguarding concern, not a behaviour issue.
- DSL assesses risk, records concerns, and involves external agencies where appropriate.
- Staff may search and delete content on devices following DfE guidance.

11 Use of Artificial Intelligence (AI)

Staff use of AI:

- Allowed for planning, resource creation, and professional tasks.
- Outputs must be checked for accuracy and bias.
- No personal or identifiable pupil data may be entered.

Pupil use of AI:

- Only under direct supervision using age-appropriate platforms.
- Pupils are taught that AI content may be inaccurate or biased, and personal information should never be shared.
- Misuse is treated as an online safety or safeguarding concern

12 Remote Learning

- Remote learning sessions are supervised.
- Expectations are set for camera, microphone, and chat use.
- Staff follow professional conduct guidance.
- Platforms are monitored for safeguarding concerns.
- Any safeguarding concerns arising during remote learning are reported and managed in line with the school's safeguarding procedures.

13 Photography, Images and Video Use

- Photographs and videos of pupils are taken, stored, and shared securely with parental consent.
- Staff must not use personal devices to capture images of pupils.

14 Acceptable Use of ICT Systems

- All users sign acceptable use agreements, reviewed regularly.
- School systems are monitored to safeguard pupils and prevent misuse.

15 Data Security and GDPR Compliance

Staff must ensure:

- Personal and sensitive data is kept secure and accessed only by authorised individuals.
- Passwords are strong, confidential, and changed regularly.
- Devices containing personal data are encrypted where appropriate.
- Personal data is not stored or transferred to unauthorised devices or platforms.
- Data breaches or concerns are reported immediately to the Headteacher or DSL and managed in line with the Data Protection Policy.

16 Reporting Channels

Pupils and staff are taught how to report online safety concerns:

- Speaking to a trusted adult (e.g. class teacher, teaching assistant, DSL)
- Senior leadership team

Pupils are taught explicitly when and why to report concerns, including situations where something makes them feel unsafe, worried, or unsure.

All reports are treated as safeguarding concerns where appropriate and are recorded and followed up in line with school procedures.

Staff may also raise concerns through safeguarding or whistleblowing procedures. All concerns are logged and followed up in line with safeguarding procedures.

Pupil voice is used to inform online safety provision, including through surveys, discussions and school council feedback.

Pupils are reassured that:

- They will be listened to
- They will be taken seriously

They will be supported

17 Responding to Misuse and Incidents

- Online safety incidents are managed proportionately and in line with school policies.
- Following incidents, the school reviews practice and may adapt procedures, provide additional support, or adjust teaching to reduce future risk.
- Serious concerns may be referred to external agencies, including the police.
- Staff may search, screen or confiscate pupils' devices where there is reasonable cause, following DfE guidance.
- Parents/carers are informed unless doing so places a child at further risk.

The school adopts a safeguarding-first approach, recognising that misuse of technology may indicate underlying vulnerability or risk.

18 Training

- All staff receive safeguarding and online safety training at induction and at least annually.
- Training includes emerging risks, new technologies, misinformation, AI, peer-on-peer concerns, and online sexual abuse.

19 Monitoring, Evaluation and Review

- The DSL reviews incident logs, evaluates online safety education, and monitors staff confidence.
- This policy is reviewed annually or sooner if guidance or risks change.

20 Linked Policies and Appendices

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements (Appendices 1 and 2)
- Incident Logging Template (Appendix 3)

Appendix 1 – EYFS/KS1 Acceptable Use Agreement

Mereside Learner Acceptable Use Agreement (Early Years/KS1)

Mereside
Church of England Primary Academy
Learn to Love, Love to Learn

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules?

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Signed (child): _____

Appendix 2 – KS2 Acceptable Use Agreement

Mereside Learner Acceptable Use Agreement (KS2)

Mereside
Church of England Primary Academy
Learn to Love, Love to Learn

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I agree to use the school's digital systems safely and responsibly to protect me, other learners and the school.

Keeping Safe Online

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.
I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner:_____ Class:_____

Signed: _____ Date:_____

Appendix 3 – Incident Logging Template

Date & Time of alert	Username/iPad number	Person/Year group identified	Theme	Actions	Follow up	Staff members involved
When the incident happened (recorded from Smoothwall)	Login details or iPad number (recorded from Smoothwall)	Using information from login/iPad number identify year group.	Theme as recorded by Smoothwall	What actions have been taken to fact find and create whole picture of alert.	Who was spoken to and what the next steps were?	Who were the staff members involved in following actions?