

Christ Church New Malden

Church of England Primary School



Online Safety Policy

Committee responsible	Governing Body
Approval required by	Headteacher
Statutory or Recommended	Statutory
Frequency of review	Every three years
Date last reviewed	July 2026
Date of next review	July 2029
Display on website	Yes
Purpose	To ensure the safety and wellbeing of children
Link with other policies	Safeguarding

	Signed	Date
Headteacher		July 2026
Chair of Governors		July 2026

1. Scope and Aims

This policy applies to everyone in our school community, including staff, governors, volunteers, pupils, parents, and visitors who use school technology or access the internet while on site.

Our aims are to:

- Keep every member of our community safe online, both in school and at home.
- Help children develop the skills they need to use technology responsibly and confidently.
- Make sure our systems are safe, secure, and reliable.
- Encourage pupils, staff, and families to report any concerns straight away so that we can put support in place quickly.

2. Key Responsibilities

Keeping children safe online is a shared responsibility. Different members of staff have specific roles:

- **Headteacher:** Approve this policy each year and has overall responsibility for online safety and ensures that our systems, filtering, and monitoring meet national requirements.
- **Designated Safeguarding Lead (DSL):** (Alex Roe – also Filtering/Monitoring Lead) Oversees all online safety concerns and works closely with families, staff, and outside agencies when support is needed.
- **Online Safety/Website & Social Media Lead:** (Andrew Burkinshaw) Oversees our website, school social media, and how the school is represented online.
- **Network Manager:** (Lucas Roberts) Ensures our technical systems are safe, secure, updated, and appropriately filtered.

3. Managing Risk – The Four Cs

We teach children that online safety covers four main areas:

- **Content:** Making sure children do not see harmful or inappropriate material.
- **Contact:** Staying safe when communicating with others online and knowing what to do if something feels unsafe.
- **Conduct:** Understanding how our behaviour online affects others, including issues such as bullying or sharing images.
- **Commerce:** Learning about financial risks such as scams, phishing, or gambling-style games.

4. Systems, Communication Channels, and Monitoring

To keep everyone safe:

- **Messaging and Email:**
 - Pupils use school-approved platforms (e.g., Google Classroom).

- Staff only use their school email for school business.
- **Filtering and Monitoring:**
 - We use LGfL filtering to block inappropriate content.
 - School devices and accounts are monitored for safety.
 - Staff report any accidental over-blocking or gaps in filtering to the DSL and to the Network Manager
- **Generative AI:**
 - Pupils only use AI tools under adult supervision and never for assessments.
 - Staff must not enter any personal information about children into AI sites.
 - Staff always check AI-generated content carefully.
- **Passwords:**
Everyone must keep passwords private and secure.

5. Devices, Mobile Phones, and Wearable Technology

- **Pupils:**
 - CCNM is a smartphone free school.
 - Phones, smart glasses, AirTags, and recording devices are not allowed.
 - Taking photos or videos of others without permission is strictly forbidden.
- **Staff:**
 - Phones must be on silent and used only in staff areas.
 - In exceptional circumstances, staff may use a personal device to take photos on a school trip, but images must be transferred to school storage immediately and deleted from the device.
 - The Headteacher may search or confiscate a device if there is a safeguarding concern.

6. Social Media and Online Conduct

- The school's online presence is monitored to protect our community.
- Everyone is expected to behave respectfully online.
- Parents and carers are encouraged to contact the school directly with any concerns rather than posting publicly.
- Staff and pupils must not follow or friend each other on social media.
- Staff are expected to use strong privacy settings and maintain professional boundaries at all times.

7. Education and Curriculum

Online safety is taught across the curriculum, particularly in Computing, PSHE, and RSHE. We use the **Education for a Connected World** framework to guide our teaching.

Children learn about:

- Healthy relationships and consent
- Critical thinking and recognising misinformation
- Digital footprints
- Copyright and ownership
- Safe and responsible use of technology

Lessons are adapted to meet the needs of all learners, including pupils with SEND or other vulnerabilities.

8. Incident Handling and Safeguarding

All online safety concerns are treated as safeguarding matters and must be reported to the DSL on the same day. Incidents are recorded on MyConcerns.

Specific guidance:

- **Cyberbullying:** Treated in the same way as face-to-face bullying.
- **Sexual harassment or violence online:** Zero tolerance.
- **Abusive social media posts:** The school may request their removal and seek advice from the POSH Helpline.
- **Sharing of nude or semi-nude images:**
 - Staff must not view, share, or delete these images.
 - The DSL must be informed immediately.
 - We follow UKCIS national guidance to safeguard the pupil without unnecessary criminalisation.

9. Data Protection and Use of Images

- The school follows Data Protection legislation and guidance led by the DPO (Andrew Burkinshaw).
- GDPR does not prevent staff from sharing information needed to keep children safe.
- Parental consent for photographs is collected when children join the school.
- When pupils appear in public materials, we use first names only.
- Staff must check consent before using any images.

10. Communication and Review

- This policy is available on the school website and in the Staff Handbook.
- Acceptable Use Policies (AUPs) are shared with staff, pupils, and parents annually or whenever updated.
- The policy is reviewed each year or sooner if guidance or technology changes.

Appendix A – Roles and Responsibilities

1. All Staff

- Sign and follow the Staff Acceptable Use Policy.
- Report any concerns—no matter how small—to the DSL immediately.
- Model safe and respectful online behaviour.
- Avoid language that blames victims in online incidents.
- Supervise pupils closely when using technology.
- Report any issues with filtering to the DSL.

2. Headteacher (Neil Meehan)

- Embeds online safety into the culture of safeguarding.
- Ensures all staff receive regular training.
- Oversees filtering, monitoring, and data protection systems.
- Ensures an annual online safety audit is completed.

3. Designated Safeguarding Lead – Alex Roe

- Leads on all online safety matters.
- Works closely with the Network Manager to maintain safe systems.
- Logs and follows up all online incidents.
- Ensures online safety is threaded throughout the curriculum.
- Keeps up to date with new risks and trends.
- Reviews this policy regularly.

4. Governing Body (Link Governor: Marcy Gwanzura/ Rob Shrimpton)

- Ensures governors receive online safety training.
- Monitors compliance with filtering and monitoring standards.

5. Curriculum Leads

- **PSHE/RSHE Lead (Nicola Brooks):** Ensures pupils learn about healthy relationships, consent, wellbeing, and relevant online risks.
- **Computing Lead (Ruth Wogan):** Oversees online safety teaching within the Computing curriculum and works with technical staff to support safe learning.

All subject leaders look for natural opportunities to reinforce key online safety messages.

6. Network Manager (Lucas Roberts)

- Manages school systems securely.
- Maintains filtering and monitoring tools.
- Ensures new devices are safe before use.

7. Data Protection Officer (Karen Churms)

- Ensures compliance with GDPR.
- Monitors access to safeguarding records.
- Supports staff in making safe decisions about information sharing.

8. Other Community Members

- **Volunteers and contractors:** Must sign the AUP and work only under school-approved arrangements.
- **Pupils:** Follow the Pupil Acceptable Use Rules.
- **Parents and carers:** Read and sign the Parent AUP and help children follow school rules at home.
- **External groups hiring the school:** Must sign an AUP and use technology responsibly.