



Christ the King Catholic Primary School

Computing and Online Safety Policy

2026-27



Christ the King Primary School

- ✦ To live & learn together in harmony.
- ✦ To grow & develop in Christ.
- ✦ To reflect God's love in all we do.

Policy review Date	September 2026
Date of next Review	September 2027
Who reviewed this policy?	Tracy Lane DSL

Policy Status: Statutory

Date Approved: September 2026

Review Date: September 2027

Designated Safeguarding Lead (DSL): Tracy Lane

Deputy DSLs: John Lane, Alice Brady, Nichola Beveridge, Alex Fernandez-Madden, Cat Le Fleming

Computing Lead: Heather Stanton

Filtering and Monitoring Lead: Tracy Lane

Contents

- 1. Policy Statement**
 - 2. Aims**
 - 3. Scope**
 - 4. Roles and Responsibilities**
 - 5. Computing Lead Responsibilities**
 - 6. Communication of this Policy**
 - 7. Understanding Online Risks**
 - 8. Online Safety Education and Curriculum**
 - 9. Artificial Intelligence and Emerging Technologies**
 - 10. Acceptable Use Agreements**
 - 11. Social Media**
 - 12. Mobile Phones and Personal Devices**
 - 13. E-mail and Electronic Communication**
 - 14. Filtering and Monitoring**
 - 15. Cyber Security**
 - 16. Data Protection and Information Security**
 - 17. Equipment, Infrastructure and Network Management**
 - 18. School Website and Published Content**
 - 19. Images, Videos and Digital Media**
 - 20. Online Safety and Safeguarding**
 - 21. Remote Learning**
 - 22. Managing Online Safety Incidents**
 - 23. Record Keeping**
 - 24. Working with Parents and Carers**
 - 25. Asset Management and Disposal**
 - 26. Monitoring and Review**
-

1. Policy Statement

Christ the King Catholic Primary School recognises that technology is central to the lives of children, families and staff and provides significant educational, social and communication opportunities. However, technology can also present safeguarding and wellbeing risks both online and offline.

Online safety is an integral part of safeguarding and child protection and forms part of the school's whole-school safeguarding approach. The school is committed to creating and maintaining a culture where children can learn, communicate and engage with technology safely, responsibly and respectfully.

The school recognises that online harms can occur through computers, tablets, mobile phones, smart watches, step tracking devices, gaming platforms, social media, messaging services, livestreaming, artificial intelligence (AI), virtual environments and emerging technologies.

This policy should be read alongside the following policies:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Data Protection Policy
- Acceptable Use Agreements
- Mobile Phone Policy
- Relationships and Health Education Policy

Any online safety concern must be treated as a safeguarding concern and managed in accordance with the school's safeguarding procedures.

2. Aims

The school aims to:

- Safeguard and promote the welfare of children online.
 - Protect children and adults from online harms.
 - Promote safe, responsible and respectful use of technology.
 - Ensure effective filtering and monitoring arrangements.
 - Deliver high-quality Computing and Online Safety education.
 - Support staff in recognising, reporting and responding to online risks.
 - Promote positive digital citizenship.
 - Support parents and carers in keeping children safe online.
 - Promote cyber security and data security.
 - Ensure compliance with Keeping Children Safe in Education 2026 and other statutory guidance.
 - Support the safe, responsible and ethical use of artificial intelligence and emerging technologies.
-

3. Scope

This policy applies to:

- All children.
- All staff.
- Governors.
- Volunteers.
- Contractors.
- Visitors.
- Parents and carers.
- External organisations using school premises.

The policy applies when technology is used:

- On school premises.
 - During educational visits.
 - During remote learning.
 - On school-owned devices.
 - On personal devices where safeguarding concerns arise.
 - Inside and outside school where behaviour may impact on the safety or wellbeing of members of the school community.
-

4. Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure the school has appropriate online safety arrangements.
- Ensure filtering and monitoring arrangements are effective.
- Review this policy annually.
- Receive safeguarding reports relating to online safety.
- Ensure sufficient resources are available to support online safety.

Executive Headteacher

The Executive Headteacher will:

- Ensure online safety is embedded within safeguarding arrangements.
- Promote a strong safeguarding culture.
- Ensure staff receive appropriate training.
- Ensure concerns are responded to appropriately.
- Work closely with the DSL and Computing Lead.

Designated Safeguarding Lead

The DSL will:

- Lead online safety across the school.
- Manage online safeguarding concerns.
- Ensure concerns are recorded appropriately.
- Oversee filtering and monitoring arrangements.
- Coordinate safeguarding responses.
- Liaise with external agencies.
- Lead the annual online safety review.
- Monitor emerging risks and trends.

All Staff

All staff will:

- Maintain an attitude that "it could happen here".
- Follow safeguarding procedures.
- Follow Acceptable Use Agreements.
- Model safe technology use.
- Report concerns promptly.
- Challenge unsafe online behaviour.
- Complete safeguarding, online safety and cyber security training.

5. Computing Lead Responsibilities

Curriculum Leadership

The Computing Lead will:

- Lead the development, implementation and review of the Computing Curriculum.
- Ensure compliance with National Curriculum requirements.
- Ensure online safety is embedded throughout the curriculum.
- Monitor teaching and learning in Computing.
- Ensure progression in digital literacy and online safety knowledge.
- Liaise with PHSE lead to ensure coverage

The curriculum will include:

- Online relationships.
- Cyberbullying.
- Social media.
- Privacy and personal information.

- Digital footprints.
- Copyright and ownership.
- Misinformation and disinformation.
- Online scams and fraud.
- Cyber security.
- Artificial intelligence.
- Deepfakes and manipulated media.
- Reporting concerns and seeking support.

Online Safety Education

The Computing Lead will:

- Support delivery of online safety education.
- Promote Safer Internet Day and awareness campaigns.
- Share emerging risks with staff and families.
- Support the annual online safety review.

Acceptable Use Policies

The Computing Lead will:

- Review and update Acceptable Use Agreements.
- Monitor implementation.
- Support investigations into breaches.

Equipment and Infrastructure

The Computing Lead will:

- Support secure configuration of devices.
- Review software and online platforms.
- Support filtering and monitoring systems.
- Promote cyber security and equipment safety.
- Ensure equipment is used safely and appropriately.

Emerging Technologies

The Computing Lead will:

- Monitor developments in technology and AI.
- Assess educational and safeguarding implications.
- Provide guidance for staff.
- Support ethical and safe use of technology.

Professional Development

The Computing Lead will:

- Support staff training.
- Share updates and guidance.
- Promote best practice across the curriculum.

Parental Engagement

The Computing Lead will:

- Support parental awareness programmes.
- Share online safety information.
- Promote online safety resources.

6. Communication of this Policy

This policy will be communicated through:

- Staff induction.
- Annual safeguarding training.
- School website publication.
- Parent communications.
- Acceptable Use Agreements.
- Staff meetings.
- Governor updates.
- Computing curriculum activities.

7. Understanding Online Risks

The school recognises four broad areas of online risk.

Content

Children may encounter:

- Pornography.
- Violent content.
- Racist material.
- Extremist content.
- Misogynistic content.
- Self-harm and suicide content.
- Misinformation.
- Disinformation.
- Harmful online challenges.
- AI-generated harmful content.

Contact

Risks include:

- Grooming.
- Radicalisation.
- Exploitation.
- Harmful advertising.
- Fraud.
- Manipulation.
- Adults posing as children.

Conduct

Risks include:

- Cyberbullying.
- Harassment.
- Child-on-child abuse.
- Sexual harassment.
- Sharing of nude or semi-nude images.
- Hate-based behaviour.
- Misogyny.
- Harmful online behaviours.
- Abuse using emerging technologies.

Commerce

Risks include:

- Gambling.
- Scams.
- Phishing.

- Financial exploitation.
 - In-app purchases.
 - Commercial pressures.
-

8. Online Safety Education and Curriculum

Online safety is embedded throughout:

- Computing.
- PSHE.
- Relationships Education.
- Health Education.
- Assemblies.
- Safeguarding activities.

Children will be taught:

- Safe internet use.
 - Healthy online relationships.
 - Respectful online behaviour.
 - Digital wellbeing.
 - Privacy and security.
 - Consent online.
 - Social media awareness.
 - Image sharing.
 - Gaming safety.
 - Livestreaming safety.
 - How to report concerns.
 - Artificial intelligence awareness.
 - Deepfakes.
 - Misinformation and disinformation.
-

9. Artificial Intelligence and Emerging Technologies

The school recognises that AI presents both opportunities and safeguarding risks.

Pupils will learn:

- What AI is.
- How AI-generated content is created.
- How to identify deepfakes and manipulated media.
- How to verify online information.
- How to use AI responsibly.

Staff will:

- Use AI ethically and professionally.
 - Consider safeguarding and data protection implications.
 - Report concerns relating to AI-generated abuse, exploitation or manipulation.
-

10. Acceptable Use Agreements

The school maintains Acceptable Use Agreements for:

- Staff.
- Governors.
- Volunteers.
- Pupils.
- Parents and carers.

All users are expected to comply with their agreement.

Failure to comply may result in:

- Removal of access.
 - Behaviour sanctions.
 - Disciplinary action.
 - Safeguarding intervention.
 - Referral to external agencies.
-

11. Social Media

Staff must:

- Maintain professional boundaries.
- Never communicate with pupils via personal social media.
- Never accept friend requests from current pupils.
- Avoid discussing school matters online.
- Protect personal information.

Pupils will be taught:

- Safe social media use.
- Privacy and security settings.
- Online reputation management.
- Respectful communication.
- Reporting concerns.

Parents are expected to use social media responsibly and follow school communication procedures.

12. Mobile Phones and Personal Devices

Christ the King operates as a mobile-phone-free school. See the CTK mobile phone policy for additional information.

Pupils

- Mobile phones should not be brought into school.
- Any agreed exception must be approved by the DSL.
- Devices brought onsite must remain switched off and securely stored.

Staff

- Personal devices must not be used to communicate with pupils.
 - Personal devices must not be used to photograph children.
 - School equipment should always be used for professional purposes.
-

13. E-mail and Electronic Communication

Staff must:

- Use school-approved systems.
- Maintain professional communication.
- Never use personal email for pupils.
- Protect confidential information.
- Follow GDPR requirements.

Pupils will be taught safe and responsible electronic communication.

14. Filtering and Monitoring

The school uses filtering and monitoring systems to protect users.

The school will:

- Filter harmful content.
- Monitor online activity.
- Investigate concerns.
- Review systems at least annually.

Concerns must be reported if:

- Inappropriate content becomes accessible.
- Filtering fails.
- Monitoring fails.
- Attempts are made to bypass controls.

15. Cyber Security

The school promotes strong cyber security practices.

Staff will:

- Complete cyber security training.
- Use strong passwords.
- Report phishing attempts.
- Use multi-factor authentication where required.
- Follow data security procedures.

Pupils will learn:

- Password security.
- Safe online behaviour.
- Fraud awareness.
- Information protection.

16. Data Protection and Information Security

The school will comply with:

- UK GDPR.
- Data Protection Act 2018.
- Safeguarding information-sharing requirements.

The school will:

- Store data securely.
- Limit access to authorised users.
- Maintain secure backups.
- Use encrypted transfers where appropriate.

Any data breach must be reported immediately.

17. Equipment, Infrastructure and Network Management

The school will:

- Maintain secure networks.
- Ensure anti-virus protection is active.
- Maintain appropriate backups.
- Restrict access to authorised users.
- Monitor network health and security.
- Maintain secure wireless access.
- Regularly review infrastructure security.

Users must never share passwords or use another person's account.

18. School Website and Published Content

The Executive Headteacher retains overall responsibility for website content.

The school will:

- Ensure information is accurate.
 - Meet statutory publication requirements.
 - Protect children's identities.
 - Regularly review published content.
 - Ensure safeguarding considerations are applied to all online content.
-

19. Images, Videos and Digital Media

The school will:

- Obtain parental permissions.
- Protect children's privacy.
- Avoid publishing full names with images.
- Securely store digital media.
- Regularly review online content.

Pupils will be taught:

- Image consent.
 - Safe image sharing.
 - Privacy and security.
-

20. Online Safety and Safeguarding

Online abuse is a safeguarding concern.

Examples include:

- Grooming.
- Sexual exploitation.
- Criminal exploitation.
- Online sexual harassment.
- Cyberbullying.
- Radicalisation.
- Image-based abuse.
- Deepfake abuse.
- AI-enabled abuse.

All concerns must be reported immediately to the DSL.

21. Remote Learning

Staff must:

- Use approved platforms.
- Maintain professional boundaries.
- Record concerns appropriately.
- Avoid private communication.
- Ensure they have added Computing Lead to Google Classrooms for safeguarding and monitoring purposes.

Children must be protected from inappropriate online content during remote learning.

22. Managing Online Safety Incidents

All online safety incidents will be taken seriously.

Staff must:

- Record concerns on CPOMS.
- Inform the DSL.
- Preserve evidence.
- Not investigate independently where safeguarding concerns exist.

The school may seek support from:

- Children's Social Care.
- Police.
- CEOP.
- Internet Watch Foundation.
- Local Authority.
- Prevent Team.
- UK Safer Internet Centre.

23. Record Keeping

Online safety concerns will be recorded on CPOMS.

Records will include:

- Nature of concern.
- Actions taken.
- Advice received.
- Outcomes.
- Follow-up actions.

The DSL will regularly review records for patterns and emerging concerns.

24. Working with Parents and Carers

The school will:

- Promote parental awareness.
- Provide guidance and resources.
- Share online safety updates.
- Offer information sessions where appropriate.
- Support parents in managing concerns.

Parents are encouraged to:

- Monitor online activity.
 - Discuss online safety regularly.
 - Report concerns promptly.
 - Support positive digital behaviour.
-

25. Asset Management and Disposal

The school maintains inventories of:

- Hardware.
- Software.
- Digital assets.

When equipment is disposed of:

- Data will be securely erased.
 - Storage media will be wiped or destroyed.
 - Disposal will comply with environmental and data protection requirements.
-

26. Monitoring and Review

This policy will be reviewed annually or sooner if:

- Legislation changes.
- New technologies emerge.
- Significant incidents occur.
- Local safeguarding arrangements change.

The annual review will include:

- Filtering and monitoring effectiveness.
 - Online safety incidents.
 - Curriculum provision.
 - Staff training.
 - AI developments.
 - Cyber security.
 - Acceptable Use Agreements.
 - Parent engagement.
 - Pupil voice.
-

This policy should be read alongside the school's Safeguarding and Child Protection Policy and forms part of the school's wider safeguarding framework.