St Cuthbert's
ROMAN CATHOLIC ACADEMY TRUST

Online Safety Policy

Name and Job Title of Author:	Nicola Spray, Director of Safeguarding
Approval Committee:	Directors
Date policy approved:	Autumn 2025
Version number:	v.1
Target Audience:	All
Date of next review:	September 2026

ENCOUNTER • LEARN • GROW • FLOURISH

Table of changes

Version Number	Date of Version/Review	Detail changes
V1	Autumn 2025	

Contents

1. Statement of intent
2. Legal framework
3. Roles and responsibilities
4. Managing online safety
5. Cyberbullying
6. Sexual Violence and Sexual Harassment between Children (Includes Critical Protocol)
7. Grooming and exploitation
8. Mental health
9. Online hoaxes and harmful online challenges
10. Cyber-crime
11. Online safety training for staff
12. Online safety and the curriculum
13. Use of technology in the classroom
14. Use of smart technology (Mobile Phones)
15. Educating parents
16. Internet access
17. Network security (Cyber Essentials)
18. Emails (Cyber Response & Backups)
19. Generative artificial intelligence (AI)
20. Social networking
21. School websites
22. Use of devices
23. Monitoring and review (SARs)

Statement of intent

St Cuthbert's Roman Catholic Academy Trust understands that using online services is an essential aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online

services is embedded throughout the trust; therefore, several controls are in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. The trust has created this policy to ensure appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance, including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (Current Statutory Guidance) 'Keeping children safe in education'
- DfE (2023) 'Teaching online safety in school'

- DfE (2022) 'Searching, screening and confiscation'
- DfE (2025) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World-2020 edition.
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (NCSC) 'Cyber Essentials Requirements'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- IT Acceptable Use Agreements
- Anti-Fraud and Corruption policy (includes Cyber element)
- Information Security Policy
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Social Media Policy

For any concerns regarding data privacy, breaches, or SARs, please contact the Data Protection Officer (DPO)

Name: Sophie Teasdale

Email: steasdale@scrcat.org

Telephone: +44 1482851136

2. Roles and responsibilities

The Board of Directors / Local Governing Boards will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Leads' (DSLs) remit covers online safety.
- Review this policy annually or following any significant national updates or local incidents.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at least annually thereafter.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually, documenting this review in Board minutes, in liaison with the IT Managed Service Provider.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, manage them effectively, and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have a practical approach to planning for and responding to online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The headteacher will be responsible for:

- Ensuring that online safety is a consistent and interrelated theme throughout the school's policies and procedures, including those related to the curriculum, teacher training, and safeguarding.
- Supporting the DSL and the Deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and IT Managed Service Provider.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training provided to staff includes an understanding of the expectations, roles, and responsibilities related to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.

The IT Managed Service Provider (MSP) will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and well-being issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that robust processes are in place to handle any concerns about pupils' online safety. The DSL should liaise with the police or children's social care services for support in responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive annual training, with updates provided at least on a termly basis.
- Staff receive at least termly email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into the learning curriculum throughout.

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask that no one be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary to protect them from further harm. Ultimately, the DSL will balance the victim's wishes against their duty to protect the victim and other young people.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips are sent via mobile phone cameras.
- Silent or abusive phone calls.
- Threatening or bullying emails.
- Unpleasant messages are sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse.
- Discriminatory bullying online, i.e. homophobia, racism, misogyny/misandry.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

5. Sexual Violence and Sexual Harassment between Children

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, offline and online.

The following are examples of online harmful sexual behaviour, of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence.

- Upskirting.
- Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.

Handling Youth-Produced Sexual Imagery ("Sexting")

Staff will be aware that creating, possessing, and distributing indecent imagery of other children (individuals under 18) is a criminal offence. To protect staff from liability and preserve the chain of evidence, the following **CRITICAL PROTOCOL** applies immediately upon discovery:

1. **DO NOT** view the image more than is necessary to verify its nature.
2. **DO NOT** forward, copy, print, or upload the **image file** to **any** cloud platform (including **CPOMS**, Google Drive, or email). Uploading indecent imagery to a server constitutes "making" an indecent image and is a criminal offence.
3. **DO: Record the details of the incident** (date, time, nature of concern, individuals involved) on CPOMS/MyConcern, but **NEVER attach the image file itself.**
4. **DO NOT** ask the child to send the image to you.
5. **DO:** Confiscate the device immediately, switch it off (or disconnect from the network), **ensure no content is deleted by the pupil or staff,** and hand it **physically** to the DSL.
6. The DSL will then consult with the police and/or children's social care in line with the *Child Protection and Safeguarding Policy*.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- They are secretive about how they are spending their time online.

- Having an older boyfriend or girlfriend, usually one who does not attend the school.
- Having money or new possessions that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Where staff have any concerns about pupils in relation to CSE or CCE, they will bring these concerns to the DSL without delay.

Radicalisation - Children who are targets for radicalisation are likely to be groomed by extremists online.

Staff members will be aware of the factors which can place confident pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy.

7. Mental health

Staff will be aware that online activity, both in and outside of school, can have a substantial impact on a pupil's mental well-being. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

"Online hoaxes" are deliberate lies designed to spread misinformation and alarm. "Harmful online challenges" involve users recording themselves engaging in risky activities.

Where staff suspect that a harmful online challenge or hoax may be circulating among pupils in school, they will report this to the DSL immediately. The DSL will conduct a case-by-case assessment.

Before deciding how to respond, the DSL and headteacher will ensure any response does not inadvertently encourage pupils to view the hoax or challenge where they would not have otherwise come across it (The "Non-Amplification" principle).

9. Cyber-crime

Cybercrime is a criminal activity that involves the use of computers and/or the internet.

- **Cyber-enabled:** Crimes carried out at higher scales online (e.g. fraud).
- **Cyber-dependent:** Crimes that can only be carried out online (e.g. hacking).

Where there are any concerns about a pupil's use of technology and their intentions about using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cybercrime and divert them to a more positive use of their skills.

10. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety. Staff training will focus specifically on harmful online narratives, including misinformation, disinformation, and conspiracy theories. Staff will also be guided on how to embed online safety themes across the wider curriculum.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum, particularly in RSHE, PSHE, Citizenship, and IT. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely, covering the 4Cs:

- **Content Risks:** Evaluating content, fake news, and radicalisation.
- **Contact Risks:** Peer pressure, grooming, and unsafe interactions.
- **Conduct Risks:** Personal behaviour, "sexting", and cyberbullying.
- **Commerce Risks:** Online gambling, scams, and phishing.

12. Use of technology in the classroom

Before using any websites, tools, apps, or other online platforms in the classroom, the class teacher will review and evaluate the resource to ensure its suitability for the school. Pupils will be supervised when using online materials during lesson time.

13. Use of smart technology (Mobile Phones)

While the trust recognises that the use of innovative technology can have educational benefits, there are associated risks.

Mobile Phone Policy

- **Trust Default (Classroom Ban):** Pupils are **not permitted** to use smart devices or any other personal technology whilst in the classroom to ensure learning is not disrupted.
- **Sanctions:** Where there is a significant problem with the misuse of innovative technology, the school will discipline those involved in line with the Trust's *Behaviour Policy*.
- **Headteacher Discretion:** Headteachers retain the full authority to implement stricter **site-wide bans** (e.g., "Gate-to-Gate") where deemed necessary to maintain order and safety or to address specific behavioural trends within their academy. Headteachers instituting gate-to-gate bans must ensure appropriate risk assessments regarding pupil travel safety are in place.

14. Educating parents

Schools will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children.

15. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the IT Acceptable Use Agreement.

16. Filtering and monitoring online activity

The Board of Directors will ensure the trust's IT network has appropriate filtering and monitoring systems in place, meeting the DfE's 'Filtering and monitoring standards for schools and colleges'.

The Headteacher and MSP will conduct a risk assessment to determine the necessary filtering and monitoring systems in place. Deliberate breaches of the filtering system will be reported to the DSL and MSP.

17. Network security (Cyber Essentials)

The Trust aligns its technical security standards with the **Cyber Essentials** framework. The MSP and SLT digital lead are responsible for implementing these measures, which include:

- **Firewalls:** Ensuring internet gateways are supported by firewalls to secure the network.
- **Secure Configuration:** Managing computers and network devices to reduce the level of inherent vulnerabilities.
- **User Access Control:** Utilising unique usernames, strong passwords, and **Multi-Factor Authentication (MFA)** to protect user accounts and data.
- **Malware Protection:** Ensuring anti-virus and malware protection is active and updated on all devices.
- **Patch Management:** Keeping software, apps, and operating systems up-to-date and patched against known vulnerabilities.

18. Emails (Cyber Response & Backups)

Access to and the use of emails will be managed in line with the Data Protection Policy and IT Acceptable Use Agreements.

Cyber Response & Backups

Any cyberattacks initiated through email will be managed in accordance with the Trust's Cyber Response and Recovery Plan, which is maintained by the Trust's IT lead.

- **Data Breach Reporting:** High-risk personal data breaches (including those resulting from cyber-attacks) must be reported to the Information Commissioner's Office (ICO) within 72 hours of the Trust becoming aware of the breach.
- **Backups:** The Trust maintains **immutable offline backups** to ensure resilience against ransomware and other cyber threats.

19. Generative artificial intelligence (AI)

Schools will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI, and how to use them safely.

- **Safety & Filtering:** Schools will limit access to harmful or inappropriate content through generative AI where technically feasible, emphasising supervision and education.
- **Academic Integrity:** The Trust recognises the risk of AI being used to produce coursework. Any AI-generated work submitted by a pupil as their own, without an appropriate declaration or permission, will be treated as **academic malpractice** and dealt with under the relevant behaviour and examination policies.
- **Data Protection:** Schools will strictly prohibit the entry of personal, sensitive, or copyrighted data into generative AI tools unless the DPO has approved a specific tool-level Data Processing Impact Assessment (DPIA).

20. Social networking

The use of social media by staff and pupils will be managed in line with the trust's Social Media Policy.

21. School websites

Headteachers will be responsible for the overall content of the school's website, ensuring it is appropriate, accurate, up-to-date, and meets government requirements. This will be supported centrally with Trust oversight.

22. Use of devices

Staff members and pupils will be issued with school-owned devices to support their work, as needed. Requirements around the use of school-owned devices can be found in the trust's Device User Agreement/Acceptable Use Policy.

The use of personal devices on school premises for schoolwork purposes will be managed in accordance with the IT Acceptable Use Policy. We also have a BYOD (Bring Your Own Device) agreement, which is distributed to Sixth Form students to manage their specific device usage.

23. Monitoring and review

The Board of Directors, the Director of Safeguarding, and the MSP will review this policy in full on an annual basis, as well as following any online safety incidents.

Subject Access Requests (SARs) - Requests for access to personal data (including chat logs or emails involving safeguarding concerns) will be handled in accordance with the Data Protection Policy. Where a request involves third-party data (e.g., data from other students), redaction procedures will be applied to protect the rights of those individuals.