

Archbishop Cranmer C. of E. Academy



'Striving for Life in All its Fullness' John 10:10

Online Safety Policy

Reviewed by: Headteacher	September 2026
Approved by: Governing Body (if applicable)	Autumn 2026
Date for next review (or earlier should legislation require it)	September 2027

Our Christian Vision: Jesus said 'I have come that they may have life in all its fullness' John 10:10.

At Archbishop Cranmer C of E Primary Academy we strive for life in all its fullness, for all our children, staff and school community.

Our Mission Statement

- **For Life in all its Fullness for today...**
 - Archbishop Cranmer is a small, caring Church of England Primary School in Aslockton, Nottinghamshire. We are a family community with Christian Values at the heart, where adults and children genuinely care for one another.
 - We **aspire** to be a high achieving school that provides an outstanding education and **community of opportunity** for all.
 - We believe that every child is unique and valued by God, with their **profound personal development** being at the heart of all we do.
 - We provide a rich and stimulating curriculum that inspires and challenges all to achieve.
 - We foster warm partnerships with parents, the local community, St Thomas's church and local charities.
- **For Life in all its Fullness for the future...**
 - We teach our children to be excellent Christian role models for the future world.
 - We are inclusive, respectful and celebrate global diversity.
 - We provide excellent care, guidance and support to enable our children to keep themselves happy, healthy and safe in their adult lives.
 - We educate children on the importance of their well-being today and in their future.

Our Christian Ethos

Archbishop Cranmer C of E Primary Academy strives to be an inclusive community where children grow, learn and achieve together. Our Take Care Learning Behaviours, held together by our Christian Values, form the essence of our ethos and gives our school its sense of value and drive. We always challenge our school community to consider what our values mean to them. Our Take Care Hand reminds us that we are always:

- Taking Care (forming meaningful relationships with ourselves and others)
- Aspiring to have a go (being creative and curious)
- Acting with Integrity (always doing the right thing)
- Working hard (aspiring to be the best we can be by embracing high challenge, creative work)
- Being proud of ourselves (growing in confidence, knowing what is possible)

We are committed to fostering a nurturing, supportive, and safe environment where every child can thrive. Our Take Care Learning Behaviours are rooted in our Christian values and prioritise mental health and wellbeing as fundamental to achieving a culture of respect, responsibility, and resilience.

Through our vision of creating a 'Culture and Community of Opportunity and Ambition,' we empower all learners to 'Strive for life in all its fullness' (John 10:10). Our behaviour policy reflects these principles, ensuring that all children have access to a broad and balanced curriculum within a framework of consistent, fair, and inclusive behavioural expectations.

Our online safety vision

We want children to be safe, discerning and responsible users of technology. Online safety is an integral part of safeguarding and is taught through the curriculum, assemblies and pastoral provision. We recognise that technology changes rapidly and that safeguarding practice must respond to emerging risks including generative artificial intelligence (AI), manipulated or synthetic content and new forms of online abuse.

Key academy roles

Headteacher / Designated Safeguarding Lead (DSL)	Mrs Melanie Stevens
Deputy DSL / SENCO / Designated Teacher for LAC and PLAC / Senior Mental Health Lead	Mrs Eleanor Hodgson
Deputy DSL / Online Safety Lead	Miss Ell Robinson
Safeguarding Governor	Dr Amy Taylor
Chair of Governors	Dr Richard Bullock
IT support provider	RM Education
Safeguarding recording system	CPOMS

Contents

1. Scope and statutory context
2. Policy development, monitoring and review
3. Roles and responsibilities
4. Acceptable use
5. Reporting and responding to concerns
6. Online safety education
7. Learner voice
8. Staff and volunteers
9. Governors
10. Families
11. Technology
12. Filtering and monitoring
13. Technical and cyber security
14. Mobile technologies
15. Social media
16. Digital images and video
17. Online publishing
18. Generative AI
19. Data protection
20. Impact and review

Appendix 1 – Legislative and guidance framework

Appendix 2 – Technical Security Standard

Appendix 3 – Filtering and Monitoring Standard

Appendix 4 – Mobile Phones and Smart Watches Standard

1. Scope and statutory context

This policy sets out Archbishop Cranmer C of E Primary Academy's approach to safeguarding members of the school community when using digital technology and online services. It should be read alongside the **Aspire & Shine Education Trust safeguarding, behaviour, data protection and staff conduct policies and the academy safeguarding addendum.**

The policy applies to staff, pupils, governors, volunteers, parents and carers, visitors, contractors and community users who access academy digital systems or use personal technology on the academy site where permitted. The academy follows Keeping Children Safe in Education 2026. Online safety is treated as part of safeguarding rather than as a separate technical issue. Our approach addresses the four broad areas of online risk: content, contact, conduct and commerce.

We recognise emerging risks including generative AI interactions, AI-generated or manipulated content, deepfakes, non-consensual intimate imagery, online misogyny and misandry, financially motivated sexual extortion ('sextortion'), misinformation and disinformation.

2. Policy development, monitoring and review

The policy is led by the Headteacher/DSL with the Deputy DSLs and Online Safety Lead. It is informed by safeguarding incidents, CPOMS records, pupil voice, curriculum review, filtering and monitoring information, advice from RM Education and national guidance.

- The policy is reviewed at least annually and earlier where guidance, technology, academy practice or risk changes.
- Filtering and monitoring provision is formally reviewed at least once each academic year.
- The annual filtering and monitoring review involves senior leadership, the DSL, RM Education and the responsible governor and records actions arising.
- Additional checks are undertaken following a safeguarding incident, significant system change or identified risk.

3. Roles and responsibilities

Headteacher and senior leaders

- Maintain a culture in which online safety is understood as part of safeguarding.
- Ensure staff understand reporting routes and receive appropriate training.
- Work with the DSL, Online Safety Lead, governors and RM Education on filtering, monitoring and cyber security.
- Ensure risks arising from new technology and generative AI are assessed before school-wide use.

Governors

- Provide strategic oversight and assurance that appropriate filtering and monitoring systems are in place.
- Receive anonymised safeguarding and online safety information.
- Ensure filtering and monitoring provision is reviewed and recorded at least annually.
- Undertake appropriate safeguarding, online safety and cyber-security awareness training.
- Dr Amy Taylor is the safeguarding governor and will provide governor oversight of online safety and filtering and monitoring.

Designated Safeguarding Lead and Deputy DSLs

- The DSL has lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place.
- The DSL team receives appropriate safeguarding and online safety updates and understands the additional online risks faced by vulnerable pupils including pupils with SEND.
- Online safety incidents with a safeguarding dimension are recorded on CPOMS and managed under safeguarding procedures.
- The DSL liaises with RM Education and external agencies where required.

Online Safety Lead – Miss Ell Robinson

- Works closely with the DSL team and leads the development of online safety practice and education.
- Ensures staff understand how to report online safety incidents and emerging risks.
- Supports curriculum leaders so that online safety is planned, progressive and responsive to current risks.
- Liaises with RM Education and supports review of filtering and monitoring arrangements.

RM Education

RM Education remains the academy's IT support provider and has technical responsibility for maintaining the academy's technical infrastructure and supporting filtering, monitoring and cyber-security arrangements.

- Maintain and support filtering and monitoring systems and provide relevant reports and technical advice.
- Support checks, risk identification and annual review with academy leaders.
- Maintain secure access controls, updates, endpoint protection and other agreed technical safeguards.
- Escalate technical concerns or evidence of misuse promptly to the DSL/senior leadership team.

4. Acceptable use

All users are expected to use academy technology safely, lawfully and professionally. Staff and volunteers must read and sign the relevant Acceptable Use Agreement. Pupils are taught age-appropriate expectations and these are reinforced through the curriculum.

- School systems and accounts must be used in accordance with academy and Trust policies.
- Staff communication with pupils and parents must use authorised professional systems.
- Users must not deliberately access, create, store or share illegal, harmful or inappropriate content.
- Passwords and authentication details must not be shared.
- Use of generative AI must comply with academy expectations, data protection requirements and safeguarding controls.

5. Reporting and responding to concerns

Online safety concerns may arise inside or outside school. Where an incident affects a pupil or the academy community it will be considered under safeguarding and/or behaviour procedures as appropriate.

- Staff must report safeguarding concerns immediately to Mrs Melanie Stevens, Mrs Eleanor Hodgson or Miss Ell Robinson and record the concern on CPOMS.
- A CPOMS entry does not replace speaking directly to a DSL where there is immediate or significant risk.
- Pupils are taught that they can speak to any trusted adult. Worry boxes are also available in classes.
- Where illegal content or serious harm is suspected staff must not conduct their own investigation, ask leading questions or unnecessarily view, copy, forward or download harmful material.
- Evidence should be preserved only in accordance with safeguarding advice and police or specialist guidance.
- Concerns about a member of staff are managed under the Trust safeguarding/allegations procedures. Concerns about the Headteacher are referred to the Chair of Governors and Trust in accordance with those procedures.

Specific online harms

Staff should be alert to online bullying, sexual harassment, grooming, exploitation, radicalisation, hate and discriminatory content, self-harm and suicide content, fraud, extortion, harmful challenges, non-consensual imagery, AI-generated or manipulated imagery and audio, deepfakes and harmful interactions with generative AI systems.

6. Online safety education

Online safety is taught through the computing curriculum and wider curriculum including relationships, health education and safeguarding education. Teaching is age appropriate, revisited and adapted to emerging risks.

- iLearn2 provides planned computing and online safety learning.

- Online safety is reinforced through assemblies, pastoral provision, Safer Internet Day, Anti-Bullying Week and responsive teaching.
- Pupils are taught to evaluate online information and recognise misinformation, disinformation, manipulation and synthetic or AI-generated content.
- Pupils learn about privacy, consent, respectful online relationships, reporting routes and the risks of sharing images and personal information.
- Teaching is adapted for pupils with SEND and other vulnerabilities where necessary.

7. Learner voice

The academy uses pupil voice, Pupil Parliament and other leadership opportunities to understand pupils' experiences of technology and to evaluate online safety provision. Pupils are encouraged to contribute to safe-use expectations and awareness activities.

8. Staff and volunteers

All staff receive safeguarding and online safety training as part of annual safeguarding training and induction. All staff read Part One of Keeping Children Safe in Education 2026 in full and sign the academy's safeguarding compliance record.

- Staff understand the four areas of online risk and emerging risks associated with AI and manipulated content.
- Staff understand filtering and monitoring arrangements and know how to report concerns about blocked or unblocked content.
- Staff model safe, responsible and professional use of technology.
- Volunteers are subject to appropriate safeguarding checks and receive information proportionate to their role.

9. Governors

Governors receive safeguarding and online safety information sufficient to provide assurance and challenge. The safeguarding governor participates in the annual filtering and monitoring review and reports assurance to the governing body.

10. Families

The academy supports parents and carers to understand online risks through communications, the academy website, information sessions where appropriate and national/local online safety resources. Families are encouraged to reinforce age-appropriate boundaries, reporting routes and safe technology use at home.

11. Technology

The academy works with RM Education to ensure its network, devices and services are as safe and secure as reasonably possible. Technical safeguards do not replace education, supervision or professional judgement.

12. Filtering and monitoring

Filtering and monitoring are core safeguarding controls. The academy follows the DfE filtering and monitoring core standard and works with RM Education to ensure provision reflects the age, needs and risk profile of pupils and staff.

- Filtering applies to academy-managed devices and users accessing the academy network as appropriate.

- No filtering system is completely effective. Staff supervision, curriculum education and clear reporting routes remain essential.
- Filtering changes and temporary exceptions must be authorised and documented.
- Monitoring arrangements must enable concerns requiring safeguarding intervention to be identified and acted on promptly.
- The academy considers whether provision can address real-time, dynamic, personalised and AI-generated content.
- Before introducing a generative AI product the academy considers safeguarding, age suitability, data protection, content moderation and the DfE generative AI product safety standards.
- The results of the annual review and any actions are documented.

13. Technical and cyber security

- RM Education provides technical support for security, patching, endpoint protection, filtering and monitoring and access controls.
- Multi-factor authentication is used for accounts with access to sensitive or personal data where supported and required.
- Users must protect passwords and report suspected compromise immediately.
- School systems, software and devices are kept updated and managed in line with DfE digital and technology standards and Trust requirements.
- Personal data must only be stored and transferred using approved secure systems.
- Cyber incidents are reported promptly to senior leaders and RM Education.

14. Mobile technologies

The academy's arrangements for mobile phones and smart watches are set out in Appendix 4 and should be read alongside the Trust mobile phone policy and academy local arrangements.

Visitors, volunteers and contractors are informed of the academy's expectations for personal devices.

15. Social media

Staff must maintain professional boundaries online and comply with the Staff Code of Conduct and Acceptable Use Agreement. Official academy social media accounts are managed through authorised processes.

- Staff must not use personal social media accounts to communicate with pupils.
- Confidential information about pupils, families, colleagues or academy business must not be shared.
- Online abuse, harassment or safeguarding concerns are reported through the appropriate academy procedure.

16. Digital images and video

- Images and recordings are taken, stored and published only for legitimate purposes and in line with consent, safeguarding and data protection requirements.
- Staff must know which pupils have restrictions relating to images.
- Pupil names and images are not combined in a way that creates unnecessary identification risk.
- Images must be stored on approved academy systems.
- AI tools must not be used to create, alter or manipulate identifiable images, video or audio of pupils or staff unless specifically approved following safeguarding and data-protection consideration.

17. Online publishing

The academy communicates through its public website, newsletters and authorised social media. Online publishing must minimise identification and safeguarding risk and comply with data protection, copyright and image-consent requirements. The academy website is managed through Juniper.

18. Generative artificial intelligence

Generative AI can support education and administration but introduces safeguarding, accuracy, intellectual property and data-protection risks. Its use must therefore be purposeful, age appropriate and subject to professional oversight.

- Staff must not enter confidential, special-category or identifiable pupil information into unapproved generative AI tools.
- Pupil use of generative AI must be supervised and consistent with age restrictions, curriculum intent and academy expectations.
- AI-generated output must be critically evaluated for accuracy, bias, harmful content and misinformation.
- The academy will assess products before adoption and consider whether supplier safeguards, moderation and age protections are appropriate.
- Any harmful AI interaction, AI-generated sexual content, deepfake, impersonation or manipulated image involving a pupil is treated as a safeguarding concern and reported immediately.

19. Data protection

Personal data is processed in accordance with current data protection law and Trust policy. Staff must use approved systems, minimise data shared and report suspected personal-data breaches promptly. Use of AI and educational technology must be considered within the academy's data-protection arrangements.

20. Impact and review

The academy evaluates the effectiveness of online safety provision through safeguarding records, behaviour and bullying information, pupil voice, staff feedback, curriculum monitoring, filtering and monitoring review and governor oversight. Learning from incidents is used to improve education, procedures and technical controls.

Appendix 1 – Legislative and guidance framework

- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- Education Act 2002 and relevant academy safeguarding duties
- Online Safety Act 2023
- Data Protection Act 2018, UK GDPR and relevant changes under the Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Communications Act 2003
- Malicious Communications Act 1988
- Protection from Harassment Act 1997
- Sexual Offences Act 2003
- Equality Act 2010
- Prevent duty guidance
- DfE Meeting digital and technology standards in schools and colleges
- DfE Filtering and monitoring: core standard
- DfE Generative AI: product safety standards
- UK Safer Internet Centre guidance

Appendix 2 – Technical Security Standard

RM Education provides technical support and management in partnership with academy leaders. Technical security arrangements will be reviewed in line with current DfE digital and technology standards.

- Access rights are role based and reviewed regularly.
- Accounts with sensitive access use appropriate authentication controls including MFA where supported and required.
- Default passwords are changed and compromised credentials are reset promptly.
- Security updates and vulnerability fixes are applied in a timely manner.
- Endpoint protection, firewall, filtering and monitoring controls are maintained.
- Backups are maintained and tested in accordance with Trust/RM arrangements.
- Software installation is controlled and licensing requirements are met.
- Users report suspected security incidents immediately.
- Cyber security is considered within academy risk management and business continuity arrangements.

Appendix 3 – Filtering and Monitoring Standard

Purpose

To provide a safe digital environment through proportionate filtering and monitoring that meets safeguarding needs without unreasonably restricting teaching and learning.

Roles

- Governing body: strategic assurance.
- Headteacher/DSL: safeguarding leadership and oversight.
- Online Safety Lead: operational online-safety coordination.
- RM Education: technical management, support, reporting and system checks.

Annual review

- A formal review should place once each academic year involving SLT, DSL, RM Education and the responsible governor.

- The review considers pupil and staff risk profiles, SEND/EAL needs, technology use, off-site use, incidents, system coverage, limitations and emerging risks.
- The review specifically considers dynamic and AI-generated content and whether current controls remain proportionate.
- Actions and decisions are recorded.

Checks

- Checks are undertaken at appropriate intervals and following significant changes or incidents.
- Checks record the device/service tested, user profile where relevant, result and action taken.
- Filtering-change requests and temporary exceptions are authorised and auditable.
- Safeguarding alerts are prioritised and escalated promptly.

Generative AI

- Any generative AI product proposed for academy use is risk assessed with reference to DfE product safety standards.
- The academy considers age suitability, moderation, privacy, data processing, harmful content, simulated interaction and the ability of existing filtering/monitoring to manage risk.

Appendix 4 – Mobile Phones and Smart Watches Standard

The welfare and safeguarding of pupils is paramount. Personal devices must not interfere with learning, professional boundaries or safeguarding.

Staff, volunteers and visitors

- Personal phones should be silent and out of sight while staff are working directly with pupils except where needed for an authorised school purpose or emergency.
- Personal devices must not normally be used to photograph or record pupils.
- The Headteacher may authorise a staff member to use a personal device to take an image for a legitimate school purpose where a school device is not reasonably available. The image must be uploaded promptly to the approved school system and deleted immediately from the personal device including any recently deleted/cloud-synchronised copy where applicable.
- Personal calls and messages should normally be dealt with away from pupils during non-contact time.
- Visitors and contractors are informed of these expectations.

Pupils

- Pupils are not permitted to use personal mobile phones during the school day.
- Where a pupil is permitted to bring a phone because of agreed travel arrangements it must be switched off and stored in accordance with academy arrangements.
- Smart watches must not be used for internet access, calls, messaging, photography or recording during the school day.
- Misuse is addressed through the behaviour policy and safeguarding procedures where appropriate.

Off-site activities

- Staff may carry phones for safety and communication on educational visits but communications with parents should normally be made through agreed school channels.

Adults accompanying trips must not photograph pupils other than their own child unless explicitly authorised within school