ONLINE SAFETY & AI POLICY

Approved by	Trust Board
Date approved	Spring 2026
Review date	Spring 2027

Contents

1. Rationale

1.1 Being on line is an integral part of all our lives: our social lives, our work lives and our education. The online world is changing and we need:

1.1.1 to protect children from harmful online content and risks in the online world.

1.1.2 to support our staff to take sensible precautions against professional reputational risks, inappropriate conduct online and potential allegations about suitability to work with children.

1.1.3 to protect the organisation from business continuity risk through cyber crime.

1.1.4 to ensure, as stewards of large amounts of public data in an entrusted sector, that we keep personal data safe.

2. Purpose of the policy (Aims)

2.1 Trustees recognise that online safety and artificial intelligence (AI) are running and interrelated themes and need to be reflected as required in a variety of relevant policies and practices.

2.2 The Trust Board has overall responsibility, and ultimate decision-making authority, for safeguaring legal compliance, for the risks to the organisation around business continuity risk, cyber risk and data protection risk. The Trust Board is the employer and sets the policy for the conduct of staff, including in relation to online conduct. The Trust sets policies for safeguarding, business risk and staff conduct through discrete policies, which also cover areas of online safety and artificial intelligence (AI).

2.3 The Trust, through its scheme of delegation, gives responsibility to schools to teach broad, well-balanced and ambitious curricula, including online and media safety through an appropriate curriculum area; in primary school through Personal Development or Relationships Education, in secondary, through Wellbeing, PSHE and SRE.

2.4 The purpose of the policy is to set out the key areas of onlinesafety and AI, to describe how the Trust fulfils its obligations, and to set the culture and ethos for online safety and recognising that modern online harms are not only influenced by individual behaviour but also by the design of online platforms and algorithms generating personalised content.

2.5 The policy aims to ensure compliance with the Online Safety Act 2023, Data Protection Act 2018 and Keeping Children Safe in Education (KCSIE) guidance.

3. Ethos

3.1 This policy recognises the Trust's commitment to keeping staff, children and young people safe online and to developing a safe and responsible culture of behaviour which enables the reduction of risk, while embracing opportunities.

3.2 The Trust recognises the benefit and value of the opportunities provided by the internet, AI and other technologies and encourages schools to foster open environments in which children and young people are encouraged to ask any questions and participate in an ongoing conversation about the benefits and dangers of the online world.

3.3 The Trust has a dual responsibility when it comes to online and AI safety: to ensure procedures keep children and young people safe, and to **teach** them about online and AI safety, in and outside of school.

3.4 The Trust wishes to ensure that all members of the community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary, disciplinary or legal action will be taken.

3.5 The Trust aims to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

3.6 It is the Trust expectation that staff and children will follow appropriate conduct requirements and acceptable use policies.

3.7 The Trust is committed to online safety security measures to protect the ICT network and facilities from attack, compromise, inappropriate use, and to protect data and other information assets from loss or inappropriate use.

4. Roles and Responsibilities

4.1 The role of the Trust Board

4.1.1 The Trust Board sets the overall overall vision and mission for online safety and AI through this policy.

4.1.2 The Trust Board has overall responsibility, and ultimate decision-making authority, for safeguarding, employment legal compliance and for protecting the organisation from business risks, including cyber risks and data protection.

4.1.3 The Trust Board exercises specific legal obligations which include online safety through the setting of trust-wide policies for Safeguarding, Data Protection, Staff Code of Conduct and Business Continuity.

4.1.4 The Trust Board, through its Scheme of Delegation, delegates responsibility for planning curriculum policy to headteachers who develop school strategy, culture and ethos and develop and propose the curriculum model, including online and media safety, which the Local Committee approve, support and challenge.

4.1.5 The Trust Board holds the CEO to account on school performance, improvement and all operational areas.

4.2 The role of the CEO and Executive Team

4.2.1 The CEO and Executive Team develop and keep under continuous review, (ensuring they include areas of online safety & AI), trust-wide policies for Safeguarding, Data Protection, Staff Code of Conduct, Business Continuity and advise the Trust Board.

4.2.2 The CEO receives reports from headteachers on school performance, improvement, curriculum, and all operational areas, they advise the Trust Board on risks to the Trust generally and where necessary, in relation to online safety and AI.

4.2.3 The CEO and Executive Team recommend systems to support individual schools to mitigate risk to the Trust generally around online safety & AI.

4.3 The role of the Standards Committee

4.3.1 Report to the Trust Board on the Trust's compliance with all statutory curriculum and reporting requirements, at trust and school level, drawing on the reports of the CEO, reporting by local committees and including reports on Safeguarding (including online safety) and the Prevent Duty.

4.4 The role of the Audit and Risk Committee

4.4.1 Receive reports and recommendations from the Executive on insurance cover for business continuity.

4.4.2 Receive and challenge annual reports from the Executive and in turn report to the Trust Board on the risks around business continuity, cyber risk and data protection.

4.4.3 Support and challenge the Executive to determine the focus for internal scrutiny audits e.g. cyber and business risk in relation to IT or safeguarding including online safety & AI.

4.4.4 Provide assurance to the Trust Board on areas of risk through internal scrutiny audits and demonstrating evidence of compliance.

4.5 The role of the Local Committee

4.5.1 Support, challenge, and have input into the school curriculum model, ensuring that children are taught about online safety and AI, and recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach might be needed for more vulnerable children, victims of abuse and some SEND children.

4.5.2 Support the Headteacher to develop and implement local school culture and ethos.

4.5.3 Local committees will review safeguarding practice and procedures in schools by appointing a designated local committee member(s), with specific oversight of the school's arrangements for safeguarding, meeting with the Designated Safeguarding Lead (DSLs) to review key duties that are being undertaken across the school in relation to all safeguarding, including online safety.

4.5.4 Named local committee members will support and challenge around online safety safeguarding risks, including online mental health and suicide risks, and online sexual violence and harassment risks to children through their assurance visits with school Designated Safeguarding Leads (DSLs).

4.5.5 Receive and challenge the termly Safeguarding Report produced by the Local Committee Designated person for Safeguarding.

4.6 The role of the Headteacher

4.6.1 Headteachers are responsible for embedding a strong culture of online safety in schools and ensure the school's local procedures are reviewed in line with trust policy, mission, vision and values and communicated to all staff and parents.

4.6.2 The Headteacher will determine the approach to the provision for online safety through the curriculum with the appropriately trained member(s) of staff.

4.6.3 In all trust schools the Headteacher retains overall responsibility for safeguarding, including online safety, within the school.

4.6.4 The Headteacher will determine clear behaviour expectations of students and pupils for online activity within school (e.g. ICT acceptable use, mobile phone policies, behaviour policies).

4.6.5 The Headteacher may nominate other members of staff to lead on online safety within safeguarding, and the teaching of online safety through curriculum planning. However, the Headteacher still retains overall responsibility.

4.6.6 The Headteacher will follow trust policies and seek HR advice in dealing with staffing conduct online.

4.6.7 Headteachers will follow trust ICT protocols, keep operational processes within trust secure ICT infrastructure, and support the measures needed to be put in place to train staff about cyber risks, data protection and their responsibilities around online safety.

4.6.8 The Headteacher will utilise trust ICT facilities for screening online searches, e.g. Smoothwall..

4.7 The Role of curriculum leaders

4.7.1 Teaching online safety should not be restricted to PSHE, Wellbeing or IT and computing lessons. Embedding key messages about staying safe online throughout the curriculum helps ensure that children of all ages are taught online safety skills.

4.7.2 Curriculum leaders responsible for developing curricula in primary school through Personal Development or Relationships Education, in secondary, through Wellbeing, PSHE and SRE should follow DfE guidance for teaching online safety in schools.

4.8 The Role of Designated Safeguarding Leads

4.8.1 Promote awareness and commitment to online safety throughout the school.

4.8.2 Be the first point of contact in school on all online safeguarding matters.

4.8.3 Advise the Headteacher on appropriate training and procedures for maintaining online safety.

4.8.4 Develop and maintain an understanding of current online safety issues, guidance and appropriate legislation through regular training.

4.8.5 Advise the Headteacher on key issues regarding online safety so that they may consider how the curriculum is adapted and how communications and signposting to staff and parents are formulated appropriately.

4.8.6 Produce anonymised case studies which demonstrate online safeguarding issues for the Governing Body Committee Member safeguarding assurance visit.

4.8.7 Monitor and review online safeguarding issues through CPOMs.

4.8.8 Monitor software which reports on search trends and blocked sites for their school.

4.8.9 Ensure that staff and pupils know the correct procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an online safety incident.

4.9 All Teachers

4.9.1 Teachers should have ongoing conversations with children about the benefits and dangers of the internet and create an open environment for children and young people to ask questions and raise any concerns.

4.9.2 Embed online safety messages in learning activities where appropriate.

4.10 All Staff

4.10.1 All trust staff have an awareness of online safety and should be aware of the Trust's policy and procedures.

4.10.2 Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.

4.10.3 Report all online safety incidents via CPOMs and as appropriate to the DSL.

4.10.4 Follow trust policies and protocols for data protection and cyber risk.

5. Safeguarding

The breadth of safegaurding issues classified within online safety is considerable. The Trust recognises that online safeguarding risks arise from both the nature of the content or interaction, as well as the design of platforms and automated feeds and these design features can repeatedly expose children to harmful material. They can be categorised into four areas of risk (Keeping Children Safe In Education):

5.1 **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, hate crime, radicalisation and extremism . This includes automated search results.

5.2 **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'. This includes automated suggestions and message prompts.

5.3 **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying) . Content promotion tools may lead to behaviours being repeated, escalated and normalised.

5.4 **Commerce:–** risks such as online gambling, inappropriate advertising, phishing and or financial scams'. This includes the risk of personalised online scams.

6. Artificial Intelligence (AI)

6.1 AI Strategy

9.1.1 Cranmer Education Trust is committed to intentionally seeking and developing AI opportunities in a purpose-driven strategic manner to address challenges and needs in our schools.

9.1.2 We are committed to developing AI strategies to empower staff, grounding AI in evidence-based practices.

9.1.3 We endeavour to use AI opportunities to reduce repetitive workload.

9.1.4 We are committed to exploring opportunities AI offers safely and securely, preserving opportunities for human judgement, input and collaboration.

9.1.5 Trust 'approved' AI software will develop over time and staff should be cautious about use of free tools that are not part of a Trust initiative.

6.2 Staff use of AI

9.2.1 Staff may use credible readiliy available AI tools for the following purposes, ensuring human oversight at all times and ensuring business sensitive information is redacted:

- Administrative tasks (e.g. generating templates, drafing general communications or summarising a document)
- Lesson planning and resources, assisting in the creation of content (must be reviewed for accuracy)
- Professional development and researching best educational practices and non-sensitive reports
- Coding and IT support (must be reviewed by IT staff)

9.2.2 Staff must not use AI tools for:

- Processing any personal or confidential information
- Safeguarding reports, HR reports, disciplinary matters or financial decisions/forecasting
- Entering organisationally sensitive information such as internal strategies, security practices or school or trust operational strategies
- Generating official communications without review
- Making any automated decision making
- Uploading student work without permission and agreement through school protocols.

6.3 Data Protection for AI

9.3.1 The Trust publish privacy notices for different groups including pupils, parents and staff. These explain when and on what lawful basis the organisation proceses personal and special category data.

9.3.2 Privacy notices are clear that any automated decisions and profiling would always be subject to human involvement, overview and intelligence.

9.3.3 If schools choose to employ approved AI tools for marking or assessment, this would always be subject to a data protection impact assessment (DPIA), would be explained to students and parents/carers and would always be subject to human oversight.

9.3.4 Do not assume privacy in any free AI tools. Providers may store data for model training.

9.3.5 Anonymisation is not a guarantee, staff should assume that all inputs could be stored or analysed.

9.3.6 Staff are responsible for ensuring that AI generated content is accurate, appropriate and free from bias.

9.3.7 Staff should be mindful of copyrighted material AI can sometimes pull through.

9.3.8 Staff should be aware of and follow JCQ guidance if the school considers AI tools for assessment.

9.3.9 All breaches should be reported immediately to the Headteacher/Business Manager.

7. Curriculum

6.1 Schools will plan curriucula which ensure that children are taught about online safety, and recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach might be needed for more vulnerable children, victims of abuse and some SEND children.

6.2 Schools will consider online safety as part of providing a progressive, broad and balanced curriculum (6th Form may cover relevant issues through tutorials). This may include covering relevant issues for schools through Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils). These will include teaching age (and other personalised) appropriate teaching about radicalisation, sexual violence, and harassment online.

6.3 Remote Learning - schools will set appropriate remote education guidelines for accessing virtual learning environments and schools will follow safe digital learning strategies which are age and context appropriate. Only trust-approved systems should be utilised (e.g. MS Teams) and personal

accounts should never be used to teach online. The school should think about consent and ensuring the parents and carers and children understand the benefits and risks of remote learning. When live-teaching, staff should asses any risks and take steps to minimise them, including cameras on or off. If a student does not want to turn their camera on, try to find out why and make sure everything is okay. Follow child protection procedures with any concerns. Maintain professional boundaries and remind students how they should behave. Make sure teaching on camera or recording is done in a neutral area where nothing personal or inappropriate can be seen or heard in the background. Consider adult to child ratios including for breackout rooms.

8. Training and Support - for staff

7.1 All staff who work with children will undertake appropriate training to equip them to carry out their responsibilities for online safety, including the increasing risk of AI enabled harms and manipulation, effectively.

7.2 All staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive regular safeguarding and child protection updates, including online safety (for example, via email, e-bulletins, staff meetings) as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

7.3 Headteachers should recognise the expertise staff build by undertaking safeguarding training and managing online safeguarding concerns on a daily basis. Opportunity should therefore be provided for staff to contribute to and shape safeguarding arrangements and training so that training reflects up to date and evolving use of technology.

7.4 Online safeguarding training for staff is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning.

7.5 In determining appropriate training for teachers to teach SRE and PSHE headteachers should make sure our teachers have enough knowledge themselves, in order to identify online safety risks as well as be able to teach it.

9. Pupil Behaviour

8.1 Schools will determine appropriate pupil online safety conduct expectations through various policies: Behaviour, ICT Acceptable Use, Anti-Bullying and reflect changing use of online technology.

8.2 Pupil online and media behaviour expectations and enforcing school policy and culture is everyone's responsibility.

8.3 The safeguarding expectation in relation to peer on peer abuse online and online sexual abuse is that it should be reported to the DSL. The Trust Safeguarding Policy should be adhered to in all instances.

8.4 Teachers Standards set out the expectation that all teachers manage behaviour effectively to ensure a good and safe educational environment and requires teachers to have a clear understanding of the needs of all pupils.

10. Parental Engagement

10.1 Schools will support and include parents and carers by sharing helpful online safety advice and resources, through communications home, through parental engagement events and through signposting on websites and social media.

10.2 Schools will engage parents asking them to understand and promote acceptable use policies with their child.

10.3 Schools will encourage parents and carers to discuss online safety concerns with their children and to show an interest in how they are using technology, and encourage them to behave safely and responsibly.

10.3 Schools will engage with parents and carers about the whole school approach to online safety, about appropriate use of social media and comments, about protecting their children and also the reputation of the school.

11. Staff Conduct

11.1 Staff conduct is set out in the Trust Staff Code of Conduct Policy and covers ICT use.

11.2 It covers communication which includes protocols for emails, tells staff that that all systems are monitored, it talks about appropriate relationships and channels to use, including social media, use of mobile devices. It talks about safeguarding, prevent duty, data protection, password security, use of own devices, use of software, copyright.

11.3 Staff conduct expectations in relation to working from home, sending emails and e-safety should follow the same expectations as working from within schools, with the highest level of security, using high levels of privacy settings and password security.

11.4 The open nature of the internet and social networking means that everyone should take active steps to protect themselves, their career and their school and the Trust reputation by taking simple precautions.

11.5 Staff should think carefully before posting information about school, trust, staff, parents, even if the account is private. The language used is important and may lead to complaints.

11.6 Staff should think about how they present themselves when posting images, for their own reputation and the reputation of the school or trust, as well as to protect themselves from allegations of unsuitability or, potentially, disciplinary action.

11.7 All emails sent from a trust account should be regarded as public, always be in a professional language and appropriate to being an employee.

12. Monitoring of systems

12.1 The Trust will do all it reasonably can to limit children's exposure to online risks from the school's or college's IT system considering the age range of the children, the number of children, how often they access the IT system and the proportionality of costs vs risk.

12.2 Central Trust ICT will work with Network Managers to ensure that appropriate filters and monitoring systems are in place at schools, they will carefully liaise with Headteachers and Safeguarding Leads to block appropriately.

12.3 ICT staff should be careful that "over-blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

12.4 Central Trust ICT will provide to school Designated Safeguarding Leads appropriate access to, and training on, software which reports on search trends and blocked sites for their school.

13. Online Safety Business Risks – Continuity, Cyber Risk, Data Protection

13.1 Business Continuity

13.1.1 The Trust Business Continuity Plan sets out the ICT recovery plan for hardware failure, site or trust-wide ICT disaster, server back-ups and data recovery.

13.1.2 The Business Continuity Policy sets the expectation that schools complete a school specific Critical Incident Plan.

13.2 Cyber Risk

13.2.1 The Trust through the RPA scheme, is covered for cyber risk costs. This cover includes a 24/7 dedicated helpline 0800 368 6378 and a dedicated email address RPAresponse@CyberClan.com available in the event of a Cyber Incident.

13.2.2 All staff must undertake NCSC Cyber Security Training each year for insurance purposes.

13.2.3 The Trust is registered with the Police CyberAlarm, connecting the Trust to the local police cyber protect team and ihas a cyber alarm software tool to monitor cyber activity and records traffic on the network without risk to personal data.

13.2.4 IT protocols and policies are overseen by Executive for compliance, business risk, operational effectiness including IT Straetgy, IT risk assurance accountability (including cyber response plan), IT infrastructure set-up, IT asset register, IT KPIs and reporting and IT strategy and improvement planning.

13.2.5 Trust Executive retain evidence about safety and security of IT systems.

13.2.6 The Trust is committed to the highest level of internet security, virus protection, and web filtering.

13.2.7 The Trust is committed to achieving Cyber Esssentials accreditation and the Audit and Risk committee will oversee the action plan for working towards it.

13.3 Data Protection

13.3.1 As stewards of large amounts of public data all trust staff need to play a part in keeping that data safe.

13.3.2 Schools are an entrusted sector and look after personal and sensitive data for thousands of people.

13.3.3 Data protection is about ensuring people can trust us to use their data fairly and responsibly. It is about the fundamental right to privacy.

13.3.4 All staff should have read and understood the Trust Data Protection Policy and complete relevant training programmes as required.

13.3.5 Email and virtual working pose E-safety risks of personal information from being disclosed to the wrong person.

14. Related Policies

14.1 This policy statement should be read alongside our Cranmer Trust policies including:

- Safeguarding and Child Protection
- Managing Allegations of Abuse
- Staff Code of Conduct
- Dignity at Work Policy
- Business Continuity
- Violence and Aggression at Work
- This policy should be read alongside school policies including:
- Curriculum
- Home Learning
- Anti-bullying
- Student ICT Acceptable Use
- Mobile Devices
- Behaviour Policy
- Mental Wellbeing