



Online Safety Policy

Approved by:	Paula Tucker	Date: 1/9/26
Review by:	15/9/27	

Contents

1. Purpose and scope
 2. Legal and statutory framework
 3. Governance, roles and responsibilities
 4. Education and engagement
 5. Filtering and monitoring
 6. Information security, cyber security and data protection
 7. Generative artificial intelligence
 8. Communications, social media and personal devices
 9. Responding to online-safety concerns
 10. Specific safeguarding incidents
 11. Training, assurance and review
 12. Related policies
- Appendix A: Exemplar Template - Online-safety incident record

1. Purpose and scope

ReFocus safeguards pupils, staff and the wider school community in their use of technology. This policy applies to school systems, networks and devices, school-managed accounts, remote education, approved cloud and AI services, personal devices used in connection with school, and online conduct that affects the welfare of a pupil or the safe operation of the school.

Online safety is a complex and interrelated safeguarding theme. It is reflected in the Safeguarding and Child Protection Policy, curriculum, staff training, acceptable-use agreements, behaviour arrangements and parental engagement.

1.1 The four categories of online risk

Content – exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme violence, misinformation, disinformation and conspiracy theories.

Contact – harmful interaction with other users or generative-AI applications that simulate interaction, including peer pressure, grooming, exploitation, scams and adults posing as children.

Conduct – online behaviour that causes or increases harm, including bullying, harassment and making, sending or receiving explicit images, including images generated or altered using AI.

Commerce – online gambling, inappropriate advertising, phishing, financial scams and other commercial exploitation.

2. Legal and statutory framework

This policy has regard to Keeping Children Safe in Education 2026 (KCSIE), the statutory Mobile phones in schools guidance effective from 1 September 2026, the Prevent duty guidance, the DfE filtering and monitoring standards updated in June 2026, and current DfE guidance on generative AI in education. It supports compliance with the Education (Independent School Standards) Regulations 2014 and the Equality Act 2010.

Personal information will be handled in accordance with the UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025. The school will also have regard to relevant communications, computer-misuse, copyright, criminal and human-rights law.

ReFocus will not assume that search, screening or deletion powers applying to maintained schools and academies automatically apply to it as an independent school. Any search of a pupil or device, confiscation, examination or deletion will follow the school's published Behaviour and Mobile Phones and Personal

Devices Policies, its contractual arrangements, consent and applicable law. Safeguarding and police advice will be obtained where required.

3. Governance, roles and responsibilities

3.1 Proprietor

The proprietor has overall strategic responsibility for safeguarding, including online safety, filtering and monitoring. The proprietor will approve this policy, receive assurance that it is implemented, ensure adequate resources and review the DfE standards with leaders, the DSL and technical support.

3.2 Headteacher and responsible senior leader

The Headteacher has operational responsibility and will designate a member of the senior leadership team (SLT) to be responsible for filtering and monitoring. The responsible SLT member will oversee procurement, document decisions about what is blocked or allowed and why, lead the annual effectiveness review, oversee reports and ensure staff understand and carry out their roles.

3.3 Designated safeguarding lead

The DSL leads on safeguarding and online safety. The DSL will understand the filtering and monitoring arrangements, review relevant reports, respond to safeguarding alerts and concerns, ensure appropriate recording and escalation, work with the responsible SLT member and technical support, and provide assurance and reports to the Headteacher and proprietor.

3.4 Technical support

Internal or contracted technical support will maintain filtering, monitoring and cyber-security systems; provide intelligible reports; complete and record checks and remedial actions; protect administrative access; and report safeguarding concerns promptly to the DSL. Technical decisions will not replace safeguarding judgement.

3.5 All staff, contractors and volunteers

All staff, contractors and volunteers follow this policy, the Staff Acceptable Use Agreement and Staff Code of Conduct provide active supervision when pupils use technology and never rely on technical controls alone. All staff know how to report harmful content, a safeguarding concern, an unreasonable restriction or a failure of filtering or monitoring and they use approved accounts, platforms, devices and services and protect credentials and information. All staff report concerns immediately to the DSL and preserve evidence without viewing, copying or forwarding suspected illegal images.

3.6 Pupils and parents/carers

Pupils will receive an accessible explanation of the Student Acceptable Use Agreement and reporting routes. Parents/carers will be informed about online learning, filtering and monitoring, mobile-phone arrangements and how to raise concerns. A pupil's inability or refusal to sign does not remove the school's safeguarding responsibilities.

4. Education and engagement

ReFocus will provide age, ability and needs appropriate online-safety education through the curriculum and wider pastoral work. Teaching will address the four categories of risk, healthy and respectful relationships, privacy, consent, harmful sexual behaviour, scams, reliable information, copyright, AI, reporting and seeking help. Teaching and support will be adapted for pupils with SEND, communication needs or other vulnerabilities.

Staff will model safe and professional behaviour. Parents/carers will receive information about emerging risks, school expectations, reporting routes and sources of support. External speakers or resources will be checked for suitability and used within the school's safeguarding arrangements.

5. Filtering and monitoring

ReFocus will maintain age and role appropriate filtering and effective monitoring that meet its safeguarding needs without unreasonable over-blocking. The arrangements will cover school managed internet connected devices and services wherever used, all relevant locations and connections, guest access and any permitted bring-your-own-device arrangements. Unmanaged personal devices will use a separate network if or where access is permitted.

Filtering will use current illegal-content blocklists, including Internet Watch Foundation and Counter Terrorism Internet Referral Unit lists, and will restrict circumvention methods such as unauthorised VPNs and proxies.

Separate access profiles will be used for pupils, staff and guests. Safe search will be enabled and locked where reasonably practicable.

Monitoring will combine appropriate technical monitoring with active in-person supervision. It will be capable of identifying users or devices and generating reports or alerts that staff can understand.

The monitoring plan will include at least weekly reports of any incidents with immediate alerts for high-risk safeguarding or malicious activity, with documented ownership, response times, action and outcome.

All users will be told that filtering and monitoring are in place. Privacy notices and log-in notices will explain monitoring as appropriate.

5.1 Reviews and checks

The responsible SLT member, supported by the DSL and technical support, will review filtering and monitoring effectiveness at least once each academic year and whenever risk, working practice, devices, services, generative-AI use, major software or network configuration changes. The review will consider pupil risk profiles, SEND, safeguarding incidents, curriculum needs, mobile and app content, off-site use, technical limitations and proportionality.

Recorded checks will confirm that controls operate on all relevant devices, user groups, locations and connections. The record will state when and by whom each check was completed, what was tested, the result and actions taken. New or materially changed devices and services will be checked before use. Failures or gaps will be investigated, risk assessed, corrected and escalated.

6. Information security, cyber security and data protection

- Users will have individual accounts, use strong unique passwords and multi-factor authentication where provided, and must not share credentials.
- Devices will be locked when unattended, updated promptly, protected against malware and used only with authorised software, storage, removable media and cloud services.
- Loss, theft, phishing, malware, unauthorised access, mistaken disclosure or a suspected data breach must be reported immediately.
- Personal and special-category data will be minimised, securely transferred and retained only as required. School information must not be placed in personal email, consumer storage or unapproved services.
- The school will complete and review data-protection impact assessments where monitoring, AI or other high-risk processing requires them, and will define access, retention and deletion for monitoring information.
- Backups, access management and incident-recovery arrangements will reflect the DfE cyber-security standards and the school's risk profile.

7. Generative artificial intelligence

- AI use must be authorised, purposeful, risk assessed and appropriate to the user's age and needs. Pupil-facing use will be closely supervised and use tools with suitable safety, filtering and monitoring features. Product age restrictions and terms must be followed.
- Personal, special-category, safeguarding, confidential or identifiable pupil information must not be entered into an unapproved AI system.
- AI output must be critically checked for accuracy, bias, safety and suitability. The member of staff using it remains responsible for the final work and professional decision.
- AI must not be used to make an automated decision about a pupil or staff member unless specifically authorised and supported by appropriate transparency, human review and data-protection arrangements.
- Copyright, intellectual-property and assessment rules apply. Pupils' or staff members' original work must not be used to train an AI model without a lawful basis or permission.
- Pupils must follow teacher instructions about permitted AI use and acknowledgement. AI must not be used for cheating, impersonation, fraud, harassment, sexualised images, deepfakes, harmful advice or circumvention of safeguards.
- Any suspected AI-related safeguarding concern, unsafe output or data disclosure must be reported immediately.

8. Communications, social media and personal devices

School business and communication with pupils must use approved accounts and platforms. Staff must not communicate with current pupils through personal social-media accounts, personal messaging services or personal email. Images or recordings of pupils must be taken, stored and shared only on authorised equipment and systems with the required consent or other lawful basis.

Official social-media activity requires authorisation, appropriate account security, moderation and records. Personal online conduct must not breach confidentiality, professional boundaries, safeguarding expectations or bring the school into disrepute.

8.1 Mobile phones and smart devices

From 1 September 2026 ReFocus will be a mobile-phone-free environment by default. Pupils will not have access to mobile phones or smart technology with equivalent communication or recording functions during lessons, movement, breaktime or lunchtime. Documented exceptions and reasonable adjustments may be made for disability, medical need, safeguarding, young-carer responsibilities or another exceptional circumstance. Detailed collection, storage, return, sanctions, searching and visit arrangements will be set out in the separate Mobile Phones and Personal Devices Policy.

Staff will not use personal phones for personal reasons in front of pupils. Limited authorised operational use, such as multi-factor authentication, may be permitted. Personal devices must not be used to photograph, record or store information about pupils.

9. Responding to online-safety concerns

Anyone may report an online concern to any member of staff. Staff must listen, reassure, avoid promising confidentiality and refer safeguarding concerns immediately to the DSL or deputy. Immediate danger will be reported to emergency services. Concerns about an adult will follow the Safeguarding and Child Protection Policy, including the procedures for allegations meeting the harm threshold and low-level concerns. The LADO will be contacted where the applicable threshold or advice requires it.

The DSL will assess risk and vulnerability, consider children in other settings, preserve relevant evidence safely, decide on parental involvement, obtain police or children's social-care advice where necessary, provide support and record decisions, actions and outcomes. Sanctions will be proportionate, consistent

with the Behaviour Policy, and take account of safeguarding, age, SEND, disability and individual circumstances.

10. Specific safeguarding incidents

10.1 Making or sharing nudes and semi-nudes

All incidents involving the making or sharing of nudes or semi-nudes require a safeguarding response, whether described as consensual or non-consensual and whether photographed, altered or generated using AI. Staff must not view the image unless unavoidable and authorised by the DSL for a recorded safeguarding reason. They must never print, copy, save, forward, request or ask a pupil to share the image. The device should be secured and the DSL informed immediately. The DSL will follow current UKCIS advice and seek police or children's social-care advice as appropriate before deletion or other action.

10.2 Suspected illegal content

Staff must not investigate, search for, copy, screenshot, print, forward or delete suspected child sexual abuse material or other illegal imagery. They will stop further access, preserve the device or system state where safe, inform the DSL immediately and follow police or specialist-agency advice. Technical staff may block access without opening or reproducing the content and must preserve audit information appropriately.

10.3 Online bullying, harassment, exploitation and hate

Online bullying, discriminatory abuse, sexual harassment, coercion, grooming, criminal or sexual exploitation, scams, hate and threats will be treated as safeguarding and/or behaviour concerns. ReFocus will act where conduct affects a pupil's welfare or the school community, even if it occurred off site or on a personal device. Support will be provided to those affected and liaison with another setting or agency will take place where needed.

10.4 Radicalisation and extremism

Concerns about terrorist or extremist content, influence or contact will be referred immediately to the DSL and managed under the Prevent duty and Safeguarding and Child Protection Policy. The DSL will obtain specialist advice and make referrals where appropriate.

11. Training, assurance and review

All staff will receive online-safety and filtering-and-monitoring training at induction, regular safeguarding updates and at least annual updating appropriate to their role. The DSL, responsible SLT member and technical support will receive role-specific and provider-specific training. Training will address reporting, AI, mobile devices, harmful sexual behaviour, data protection and current risks.

The Headteacher will review this policy at least annually, following the annual online-safety risk assessment and filtering-and-monitoring review, and sooner after significant incidents or relevant legal, guidance or technology changes.

12. Related policies

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Behaviour Policy
- Staff and Student Acceptable Use Agreements
- Mobile Phones and Personal Devices Policy (to be adopted separately)
- Data Protection Policy, Privacy Notices and Records Retention Schedule
- Whistleblowing Policy
- Anti-Bullying Policy
- SEND Policy and Accessibility Plan

- Remote Education and Educational Visits arrangements
- Complaints Procedure and staff disciplinary procedures.

Appendix A: Online-safety incident record

Date/time and reporter	
Pupil(s)/adult(s) involved	
Where/how identified	
Description of concern (do not reproduce illegal imagery)	
Immediate safeguarding action	
Filtering/monitoring or technical action	
Agencies/parents informed and rationale	
Outcome, support and sanctions	
Lessons, follow-up and policy/system changes	
DSL review and closure date	