

SAFE • RESPONSIBLE • RESPECTFUL • INFORMED

Online Safety Policy

Hindle's School of Excellence Limited

Document owner	Online Safety Lead	Approved by	Director
Version	3.0	Approval date	5 September 2026
Review cycle	Annually	Next review	September 2027
Applies to	All learners, staff, volunteers and visitors	Site	115 Rochdale Road, Bury, BL9 7BA
Safeguarding applies online Harm can occur through content, contact, conduct or commerce. Online concerns must be treated with the same urgency and professional curiosity as concerns arising face to face.			

1. Purpose and scope

Hindle's School of Excellence Limited uses technology for teaching, assessment, communication, administration and remote learning. This policy establishes how technology will be used safely, lawfully and respectfully and how online incidents will be prevented, identified and managed.

It applies to learners, staff, volunteers, contractors and visitors; to Hindle's networks, accounts, data and devices; to personal devices used for Hindle's activities; to online and remote sessions; and to online behaviour outside provision where it affects safeguarding, welfare, working relationships or the safe operation of the provision.

2. Legal and guidance framework

Hindle's will have regard, where applicable to its status and activities, to current legislation and statutory guidance including:

- Children Acts 1989 and 2004 and Children and Social Work Act 2017;
- Keeping Children Safe in Education and Working Together to Safeguard Children;
- Education Act 2002 and relevant alternative-provision requirements;
- Online Safety Act 2023;
- Data Protection Act 2018 and UK GDPR;
- Equality Act 2010;
- Human Rights Act 1998;
- Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and communications legislation;
- Prevent duty guidance and the Counter-Terrorism and Security Act 2015; and
- Department for Education filtering and monitoring and digital-technology standards.

Keeping Children Safe in Education is statutory guidance, not an "Act". References in this policy include later amendments or replacement guidance.

3. Our approach: the four areas of online risk

- Content: exposure to illegal, harmful, misleading or age-inappropriate material, including pornography, violence, self-harm, suicide, hate, extremism, disinformation and harmful AI-generated content.
- Contact: interaction with adults or peers who may bully, groom, exploit, coerce, radicalise, scam or request sexual or personal information.
- Conduct: behaviour that creates harm, including cyberbullying, harassment, image sharing, impersonation, oversharing, threatening messages and unsafe participation in online challenges.
- Commerce: gambling, in-app purchases, advertising, phishing, fraud, financial exploitation, subscription traps and other commercial risks.

Risks may overlap and can be intensified by SEND, communication needs, trauma, isolation or limited digital literacy. Support and reporting routes will be made accessible.

4. Roles and responsibilities

The Director has overall responsibility for online safety, approves systems and ensures safeguarding, data protection and cyber-security arrangements are coordinated. Joanne C. Hindle is the Online Safety Lead and senior safeguarding lead. The Online Safety Lead will review incidents, risks, training, filtering and monitoring, and report material concerns to relevant agencies or commissioners.

All staff and volunteers must follow this policy and the Staff Code of Conduct, use approved systems, maintain professional boundaries, supervise learners appropriately, report concerns promptly and complete required training. Learners must follow their Learner Code of Conduct and acceptable-use expectations. Parents/carers are encouraged to reinforce safe use and report concerns affecting their child.

5. Education and learner voice

Online safety will be taught in an age-appropriate and needs-led way through lessons, induction, reminders and responses to emerging risks. Teaching will include privacy, consent, respectful communication, reliable information, passwords, scams, copyright, reporting routes, digital footprint, healthy technology use, sexual harm and safe use of AI. Learners will be invited to say what risks they encounter and what support helps them.

6. Acceptable use

Users of Hindle's technology must:

- use only authorised accounts, services and access permissions;
- keep passwords and multi-factor authentication secure and never use another person's account;
- use respectful language and avoid bullying, harassment, hate, threats or sexualised conduct;
- protect personal and confidential information and check recipients before sending;
- respect copyright, licensing, assessment rules and intellectual property;
- not bypass security, filtering or monitoring controls, install unapproved software, introduce malware or interfere with systems;
- not seek, create, store or share illegal or harmful content; and

- report mistakes, suspicious messages, security weaknesses, harmful contact or accidental access immediately.

7. Devices, mobile phones and removable media

Hindle's device and mobile-phone rules apply throughout provision. Personal devices may only be used where authorised and must not be used to photograph, film, record or contact learners. Bluetooth, hotspots, removable media and downloads may be restricted. Confidential information must not be stored on personal devices or unencrypted removable media. Lost or stolen devices containing Hindle's information must be reported immediately.

8. Accounts, passwords and access control

- Each authorised user should have an individual account appropriate to their role; shared accounts will be avoided unless operationally necessary and controlled.
- Access will follow least-privilege principles and be reviewed when roles or placements change.
- Strong unique passwords and multi-factor authentication will be used where available.
- Staff must lock screens, sign out of shared devices and never allow learners to use staff credentials.
- Accounts will be disabled promptly when no longer required, and suspected compromise will trigger password reset and incident review.

9. Filtering and monitoring

Hindle's will use appropriate filtering and monitoring on systems and networks it controls, proportionate to age, risk, SEND, privacy and the educational need for access. The arrangements will seek to block illegal and harmful content without unreasonably restricting learning or equality of access.

The Director and Online Safety Lead will understand the systems in use, identify who receives and reviews alerts, test arrangements at least annually and after significant change, record decisions and act on concerns. Filtering is not a substitute for supervision, education or professional curiosity. Personal mobile data and off-site networks may bypass Hindle's controls; expectations and risk assessments still apply.

10. Remote and online teaching

- Use approved platforms and organisational accounts wherever possible.
- Confirm learner identity and authorised attendance; use waiting rooms, meeting controls and secure links where available.
- Staff must teach from an appropriate setting, maintain professional dress and boundaries and avoid revealing private information.
- One-to-one sessions must be scheduled, recorded in the management system and visible to or known by an authorised adult under Hindle's safeguarding arrangements.
- Do not record sessions unless there is a defined purpose, lawful basis, approval, secure storage and clear notice to participants.
- Use approved communication channels and times; do not move conversations to personal social-media accounts.

- Report unexpected persons, sexual or harmful content, threats, disclosures or safeguarding concerns immediately.

11. Social media and electronic communication

Staff and volunteers must not accept learners as contacts on personal social-media accounts, exchange private personal contact details, engage in secret or disappearing-message conversations, or communicate in a way that could blur professional boundaries. Organisational posts must be authorised, accurate and respectful and must not identify a learner without a valid permission and safeguarding check.

Bullying, harassment, impersonation, doxxing, discriminatory content or threats connected with Hindle's may be managed even when posted away from the premises. Staff should preserve evidence and report it rather than retaliate or conduct their own investigation.

12. Images, video and live streaming

Images or recordings of learners will only be made on authorised equipment for a clear purpose and with the required consent or other lawful basis. Consent must be specific, recorded and capable of withdrawal for future use. Staff will consider location data, uniforms, names, personal information and whether publication could expose a learner to risk. Images will be stored securely, retained only as long as required and deleted safely.

13. Generative artificial intelligence

AI tools may support learning and administration only when authorised and used with human oversight. Users must not enter learner records, safeguarding information, health data, passwords, unpublished assessments or other confidential/personal data into an unapproved AI service. AI output must be checked for accuracy, bias, copyright, age-appropriateness and fabricated information.

Learners must follow tutor and awarding-body rules, acknowledge permitted AI assistance and submit their own work. AI-generated sexual images, deepfakes, impersonation, bullying, fraud or attempts to evade safeguarding controls are prohibited and may require safeguarding or police referral.

14. Online sexual harassment, exploitation and imagery

Sexual comments, coercion, grooming, sexualised bullying, upskirting, sextortion, sharing intimate images without consent and creating or sharing sexual deepfakes are never acceptable. A child must not be blamed or criminalised for seeking help.

Staff must not view, copy, print, forward or ask a child to send an indecent image. Secure the device or account only where safe, preserve information without opening imagery, record what was reported and contact the DSL immediately. The DSL will follow current safeguarding guidance on sharing nudes and semi-nudes, consider police or children's social care referral, and support everyone affected.

15. Cyberbullying and harmful content

Reports will be listened to, recorded and assessed for immediate risk, safeguarding, criminality and ongoing access to the victim. Hindle's may preserve URLs, usernames, dates and screenshots where

lawful; use platform reporting and blocking tools; involve parents/carers and commissioners; request content removal; and refer to police or specialist services. Support and safety planning will be prioritised alongside proportionate behaviour action.

16. Data protection and cyber security

- Use approved secure storage and share personal data only with authorised recipients for a lawful purpose.
- Apply software and security updates promptly and maintain supported anti-malware, firewall, backup and access controls.
- Treat unexpected links, attachments, QR codes, payment requests and login prompts as potential phishing.
- Do not use public or insecure Wi-Fi for confidential work without approved protection.
- Report a data breach, misdirected email, lost device, compromised account or malware immediately under the Data Breach Plan.
- Preserve logs and evidence and follow recovery, notification and business-continuity procedures.

17. Responding to an online safety incident

1. Make the person safe, provide reassurance and address any immediate medical or emergency risk.
2. Do not promise confidentiality. Report safeguarding concerns to the DSL immediately and call emergency services if danger is imminent.
3. Preserve relevant evidence without unnecessarily viewing, copying or distributing harmful material.
4. Record the facts, the learner's own words where relevant, time, platform, account and actions taken.
5. The DSL/Online Safety Lead will assess referral to parents/carers, placing school, local authority, children's social care, police, CEOP, Ofsted, the ICO or another appropriate body.
6. Remove or restrict access where possible, support affected people and manage alleged behaviour fairly.
7. Review filtering, supervision, training, risk assessments and support plans and record learning.

18. Reporting routes

Learners should tell any trusted member of staff. Staff and volunteers must report to the DSL/Online Safety Lead: Joanne C. Hindle, telephone 07538 370518, email joanne@hindlesschoolofexcellence.co.uk. If the concern involves this person, use the Deputy DSL, the placing school or relevant local-authority safeguarding route. Immediate danger: 999. Non-emergency crime: 101. Online child sexual exploitation concerns may also be reported to CEOP. Harmful or illegal content may be reported to the relevant platform and specialist reporting service.

19. Training, monitoring and review

Online safety will form part of induction and safeguarding updates for staff and volunteers. The Director will monitor incidents, near misses, technology changes, learner voice, training completion, filtering and monitoring reports and cyber-security tests. This policy will be reviewed annually and sooner after a serious incident or material change in risk, technology, law or guidance.

20. Related policies

- Safeguarding and Child Protection Policy;
- Staff Code of Conduct and Learner Code of Conduct;
- Mobile Phone and Acceptable Use arrangements;
- Data Protection, Confidentiality and Data Breach policies;
- Photography and Media Consent procedures;
- Behaviour, Anti-Bullying and Child-on-Child Abuse policies;
- Remote Learning arrangements;
- Whistleblowing Policy; and
- Business Continuity and Emergency Management plans.

21. Approval

Online Safety Lead	Joanne C. Hindle
Telephone	07538 370518
Email	joanne@hindlesschoolofexcellence.co.uk
Approved by	Joanne C. Hindle, Director
Signature	
Approval date	5 September 2026
Next review	September 2027