Online Safety Policy

EmpowerEd North policy suite

This policy has been adopted for use from May 2026 and should be reviewed against current legal, safeguarding and commissioning requirements at least annually and whenever guidance or operational arrangements change.

Policy information	Details
Date adopted	May 2026
Review date	May 2027, or sooner following any review trigger listed in this policy
Approved by	EmpowerEd North Founder/Director
Named lead	Designated Safeguarding Lead / Online Safety Lead - Janice March
Version	Version 1.0
Owner/responsible person	Designated Safeguarding Lead / EmpowerEd North Founder/Director
Completion status	CURRENT - adopted for use from May 2026. Operational evidence and contact sheets must be kept up to date before each placement.
Operational arrangements	DSL/Deputy DSL names, approved systems register, filtering and monitoring arrangements, device ownership, image consent/storage process, remote learning arrangements and cyber security controls must be confirmed before learners use EmpowerEd North digital systems or internet access.

Immediate online safeguarding action

If there is immediate risk	Call 999 where there is immediate danger, a crime in progress, serious threat of harm, or urgent medical risk. Then inform the DSL/Deputy DSL as soon as it is safe to do so.
If an online concern arises	Report to the DSL immediately. Do not delay because information is incomplete. Record what was seen, heard, disclosed or reported and the action taken.
If sexual images or illegal content are involved	Do not copy, forward, print, save, share or repeatedly view the material. Preserve the device or evidence safely where appropriate and seek DSL/police/local safeguarding advice.
If the concern involves staff conduct	Follow the Managing Allegations and Low-Level Concerns Policy and local LADO route. Do not discuss the concern with the adult involved before advice is taken.
If systems are unsafe or unconfirmed	Do not allow learner internet access through that device, network, app, platform or venue until safeguarding, filtering, monitoring and data protection arrangements are confirmed.

1. Purpose

This policy sets out how EmpowerEd North will protect learners, staff and others when digital technology, online communication, internet access, devices, images, video, social media, artificial intelligence tools or remote learning are used in connection with EmpowerEd North provision.

Online safety is part of safeguarding. Online concerns will be responded to through the Safeguarding, Child Protection and Safer Recruitment Policy, the Staff Code of Conduct and Safer Working Practice Policy, the Managing Allegations and Low-Level Concerns Policy, and the Data Protection Policy and Privacy Notice where relevant.

2. Scope

This policy applies to EmpowerEd North directors, staff, volunteers, contractors, visiting professionals and any person working with or on behalf of EmpowerEd North. It applies across any main base, community venue, off-site learning, home/community-based support, remote learning, digital communication and publicity activity.

It applies to EmpowerEd North devices and accounts, learner-owned devices used within EmpowerEd North activities, commissioner or school-provided devices, staff devices where emergency or authorised use is unavoidable, and any venue network or internet connection used during provision.

3. Pre-start online safety requirement

No learner will use EmpowerEd North internet access, digital platforms, remote learning tools, images/video processes or online learning systems until the following have been confirmed, recorded and made available to relevant staff:

- named DSL/Online Safety Lead and Deputy DSL arrangements;
- approved devices, accounts, apps and platforms;
- who is responsible for filtering and monitoring for each device, network and venue used;
- how online safety concerns, alerts or breaches will be reported to the DSL;
- photo, video, image, publicity and consent arrangements;
- cyber security controls, including passwords, multi-factor authentication, updates and device security;
- data protection arrangements, including storage, retention and access restrictions;
- communication routes with parents/carers, placing schools, commissioners and professionals;
- remote learning arrangements, if remote learning is used.

Where a placing school, local authority, commissioner or family provides the device, account, online platform or internet connection, EmpowerEd North will agree in writing who is responsible for filtering, monitoring, alert review, incident response, data protection and parent/carer communication before the arrangement begins.

4. Legal and guidance framework

This policy is informed by the following legislation and guidance, where relevant to EmpowerEd North as a specialist, part-time, non-school alternative provision:

- Children Act 1989 and Children Act 2004;

- Keeping Children Safe in Education (KCSIE) 2025, including online safety, filtering and monitoring, child-on-child abuse, staff conduct and safeguarding expectations;
- Working Together to Safeguard Children 2026;
- Alternative provision statutory guidance, Department for Education, last updated 5 February 2025;
- DfE non-school alternative provision (AP) voluntary national standards, published August 2025;
- DfE digital and technology standards for schools and colleges, including the filtering and monitoring core standard and cyber security standards, where relevant to EmpowerEd North's systems and commissioning arrangements;
- UK General Data Protection Regulation and Data Protection Act 2018;
- Equality Act 2010 and SEND Code of Practice: 0 to 25 years;
- Prevent Duty guidance: England and Wales (2023), where relevant;

UKCIS Sharing nudes and semi-nudes advice for education settings, updated March 2024;

Teaching online safety in schools, Department for Education, updated January 2023, where relevant to curriculum and learner support;

- Information sharing advice for safeguarding practitioners, where relevant;
- local safeguarding partnership procedures and local LADO routes.

5. Principles

- Online safety is safeguarding. Harm can occur online, offline or through a combination of both.
- Learners with SEND may face increased online vulnerability because of communication needs, social isolation, anxiety, literal interpretation, reduced understanding of risk, reliance on adults, or difficulty reporting concerns.
- Digital learning must be purposeful, supervised, accessible, age-appropriate, developmentally appropriate and linked to the learner's needs and EHCP outcomes where relevant.
- Filtering and monitoring must be appropriate and proportionate to the age, profile, vulnerabilities and activities of learners.
- Staff supervision is essential, but it is not a substitute for appropriate filtering, monitoring and safe systems.
- Staff must maintain professional boundaries online and must not use personal accounts to communicate with learners.
- Safeguarding concerns must be recorded and escalated promptly, even when digital evidence is incomplete.

6. Definitions

Term	Meaning
Online safety	The safe, responsible and safeguarding-aware use of digital technology, internet access, devices, apps, communication tools, images, video, social media and online content.
Filtering	Technical or provider-based controls that restrict access to harmful, inappropriate or unsuitable online content.
Monitoring	Processes used to identify concerning online activity, alerts,

	searches, content, communication or behaviour that may indicate risk.
Official EmpowerEd North platforms	Approved accounts, apps, systems, devices or communication routes used for EmpowerEd North purposes and included in the Approved Systems Register.
Personal device/account	A device or account owned or controlled by a staff member, volunteer, contractor, learner or family and not formally approved for EmpowerEd North use.
Remote learning	Learning or support delivered using digital technology when the learner and staff member are not in the same physical location.
Artificial intelligence tools	Generative or assistive tools that can create, summarise, analyse or adapt text, images, audio, video, code or other content.

7. Roles and responsibilities

7.1 Founder/Director / Leadership Team

- ensure this policy is implemented, resourced and reviewed;
- ensure appropriate filtering, monitoring, supervision and cyber security arrangements are in place before learners use digital systems;
- approve the systems, apps, devices, communication routes and online learning tools used by EmpowerEd North;
- ensure staff receive induction and refresher training in online safety and filtering/monitoring responsibilities;
- ensure online safety is considered when agreeing placements, venues, community learning, home-based support or remote learning;
- ensure any significant online safety incident leads to review of practice, systems and risk assessment.

7.2 Designated Safeguarding Lead / Online Safety Lead

- lead on online safeguarding concerns and ensure they are recorded, assessed, escalated and shared appropriately;
- understand the filtering and monitoring arrangements in place and know how concerns or alerts are reviewed;
- liaise with placing school DSLs, local authorities, police, LADO, social care, parents/carers and other agencies where required;
- ensure online safety incidents are considered within wider safeguarding chronologies and risk assessments;
- support staff to recognise online harm, exploitation, grooming, image-based abuse, harmful sexual behaviour, cyberbullying, radicalisation, scams and coercion;
- ensure accessible online safety education is planned for learners where relevant.

7.3 Staff, volunteers and contractors

- follow this policy and the Staff Code of Conduct and Safer Working Practice Policy;
- use only approved devices, accounts, apps and platforms for EmpowerEd North work unless emergency arrangements have been authorised and recorded;
- actively supervise learner use of technology and report any concern immediately to the DSL;
- never communicate with learners through personal social media, personal messaging accounts or personal email;
- protect passwords, lock devices, use multi-factor authentication where available and report lost devices or suspected breaches immediately;
- avoid viewing, copying, forwarding or sharing illegal or sexual content and seek DSL advice immediately where such material is reported or encountered;
- model safe, respectful and professional online conduct.

7.4 Learners

Learners will be supported to use technology safely, respectfully and for agreed purposes. Expectations will be taught in an accessible way using communication methods appropriate to the learner, such as visuals, social stories, AAC, modelling, symbols, simple agreements or supported practice.

7.5 Parents/carers, placing schools and commissioners

EmpowerEd North will work with parents/carers, placing schools and commissioners to agree online safety arrangements, including device ownership, filtering/monitoring responsibility, safe communication, consent, incident notification, reporting routes and any learner-specific restrictions or vulnerabilities.

8. SEND-specific online safety considerations

EmpowerEd North recognises that learners may not show online harm through verbal disclosure. Staff must maintain professional curiosity where there are changes in presentation, dysregulation, withdrawal, new fears, avoidance of devices, increased fixation on devices, secrecy, distress after online contact, sexualised language or behaviour, unexplained money/items, absconding linked to online contact, or changes in communication.

- difficulty recognising grooming, coercion, exploitation, scams, impersonation or unsafe requests;
- literal interpretation of online messages or difficulty identifying sarcasm, pressure or manipulation;
- limited understanding of privacy, consent, image sharing, location sharing or digital permanence;
- vulnerability to bullying, prejudice-based abuse, humiliation, online dares or peer pressure;
- increased risk where social isolation makes online contact feel especially important;
- communication barriers that make it harder to report harm or explain what has happened;
- use of AAC, assistive technology or shared devices that may hold sensitive personal information;
- difficulty transferring online safety teaching into real-world or unstructured digital situations.

Staff must not assume that online distress, refusal, dysregulation, aggression, withdrawal or unusual communication is simply part of autism, disability, learning disability or sensory need. Safeguarding must be considered and the rationale recorded.

9. Filtering and monitoring

EmpowerEd North will not permit learner internet access through a device, network, app, venue or platform unless appropriate filtering and monitoring arrangements have been confirmed and recorded.

- Filtering and monitoring arrangements must be appropriate to the learner's age, developmental level, SEND profile, communication needs, vulnerabilities and planned activity.
- Each device, network and platform must have an identified responsible person or organisation for filtering and monitoring.
- Where school, commissioner, local authority or family devices are used, responsibilities must be agreed in writing before use.
- Venue Wi-Fi must not be assumed safe. Community venue internet access must be risk assessed and written assurance sought where relevant.
- Personal hotspots or mobile data must not be used for learner internet access unless approved, risk assessed and recorded.
- Staff supervision remains required whenever learners use digital technology. Supervision must be proportionate to learner need and risk.
- Filtering and monitoring effectiveness will be reviewed before first use, annually, after any incident, and whenever the venue, device, platform, staffing model or learner risk profile changes.

10. Approved systems, accounts and devices

EmpowerEd North will maintain an Approved Systems Register listing the devices, accounts, apps, platforms, communication routes and storage locations approved for use. Staff must not introduce new apps, accounts, online tools, artificial intelligence systems, cloud storage, messaging routes or publicity platforms without approval.

- EmpowerEd North accounts must use strong passwords and multi-factor authentication where available.
- Devices must be password protected, locked when unattended and kept secure during travel and community-based work.
- Operating systems, browsers, apps and security software must be kept up to date.
- Learner data must not be stored on unapproved personal devices, USB drives, personal cloud accounts or personal email accounts.
- Staff must report lost, stolen or compromised devices immediately to the leadership team and Data Protection Lead.
- Shared devices must be checked so that learner information, images, login details or browsing history are not visible to other learners.

11. Learner use of technology

Learners may use technology where it supports learning, communication, independence, regulation, accessibility, Preparing for Adulthood outcomes or safe participation. Use must be planned, supervised and risk assessed where needed.

- Learners will receive accessible online safety teaching and reminders matched to their communication and cognitive profile.
- Learners must not access internet content, apps, games, communication tools or social media unless these have been approved for the activity.
- Learners must not take images, video or audio recordings of others unless this has been explicitly agreed by staff for a defined learning purpose.

- Learner-owned devices will not normally be used during EmpowerEd North sessions unless required for communication, safety, medical, accessibility or agreed learning purposes.
- Where learner-owned devices are used, expectations will be agreed with parents/carers and, where relevant, the placing school or commissioner.
- Staff will consider whether device use is affecting regulation, safety, engagement or vulnerability and will update support plans where needed.

12. Staff use of technology and online communication

- Staff must use EmpowerEd North approved accounts and communication routes for work-related communication.
- Staff must not use personal social media, personal messaging accounts or personal email to contact learners.
- Staff must not accept, request or initiate social media contact with learners, former learners who remain vulnerable, or learner family members where this could blur professional boundaries.
- Communication with parents/carers and professionals must be professional, factual, necessary and recorded where it relates to safeguarding, attendance, incidents, learner progress or placement arrangements.
- Text messaging or instant messaging must only be used where approved for practical communication, and must not be used for sensitive safeguarding records unless there is an emergency and the communication is later transferred to the appropriate record.
- Staff must not discuss learners, families, colleagues or confidential EmpowerEd North matters on personal social media.
- Staff must report accidental contact, boundary issues, inappropriate messages, friend requests or online approaches involving learners or families.

13. Images, video, audio and publicity

Images, video and audio recordings can create safeguarding and data protection risks. EmpowerEd North will use them only where there is a clear purpose, consent/legal basis, safe storage arrangements and agreed retention period.

- Written consent and any restrictions must be recorded before images, video or audio are used for publicity, website, social media or external sharing.
- Images must not be shared publicly with full names, personal details, addresses, school placement details or information that could identify a learner's location or vulnerability.
- Personal staff devices must not normally be used to take learner images. If emergency use is unavoidable, the image must be transferred to an approved secure location and deleted from the personal device as soon as possible, with the reason recorded.
- Images must not be taken during personal care, distress, restraint, medical treatment or safeguarding incidents unless there is a clear safeguarding/medical reason, DSL oversight and secure recording route.
- Images for assessment, evidence of learning or EHCP review must be stored securely and shared only with authorised people.
- Publicity posts must be checked by an authorised person before publication and must comply with consent records.

14. Social media and website use

- Only approved EmpowerEd North accounts may be used for official publicity or communication.
- At least two authorised adults should have administrative access to official accounts where practicable, so access is not dependent on one person.
- Comments and messages on official accounts will be monitored and concerns escalated to the DSL where safeguarding risk, harassment, bullying, threats or inappropriate contact are identified.
- Direct messaging with learners through social media is not permitted.
- EmpowerEd North will not post live location details for current learner activities where this could create a safety risk.
- Staff must not use personal accounts to promote, discuss or respond to individual learner matters.

15. Remote learning and online meetings

Remote learning or online meetings will only be used where suitable, agreed and safe for the learner. It must be planned and risk assessed, particularly for one-to-one support, learners with communication needs, home-based support, or learners who may be vulnerable to online harm.

- Use only approved platforms and EmpowerEd North accounts.
- Confirm who should be present or nearby, taking account of the learner's age, capacity, communication, vulnerability and family context.
- Use professional language, dress, background and conduct.
- Consider whether a second staff member, check-in arrangement or recording of attendance is needed for safeguarding and lone working reasons.
- Recording of sessions is not routine. It may only take place where there is a clear purpose, lawful basis, information/consent arrangements, secure storage, retention period and safeguarding rationale.
- Do not use private chat functions, personal contact details or unapproved messaging routes with learners.
- Any concern arising during remote learning must be recorded and escalated in the same way as an in-person safeguarding concern.

16. Artificial intelligence and emerging technology

Artificial intelligence tools may be useful for planning, accessibility or resource creation, but they must be used carefully. EmpowerEd North will not use AI tools with learner personal data, special category data, safeguarding information, images, EHCP content or confidential records unless the tool has been approved following data protection and safeguarding review.

- Staff must not enter identifiable learner, family, staff, safeguarding, health or EHCP information into unapproved AI tools.
- AI-generated resources must be checked by staff for accuracy, bias, suitability, accessibility, age-appropriateness and safeguarding risk before use.
- Learners must not use AI tools independently unless the activity is planned, supervised, age/developmentally appropriate and risk assessed.
- AI image, audio or video tools must not be used to create, alter or share images of learners without explicit approval and appropriate consent.

- Any concern involving AI-generated sexual content, impersonation, bullying, grooming, misinformation or exploitation must be treated as an online safeguarding concern.

17. Responding to online safety concerns

Online safety concerns must be treated as safeguarding concerns where there is actual or potential harm. Staff must not investigate beyond what is necessary to establish immediate safety and preserve information for the DSL.

1. Ensure immediate safety. Call emergency services if there is immediate danger, a crime in progress or urgent medical risk.
2. Listen calmly and avoid leading questions. Allow the learner to communicate in their own way, including AAC, visuals, writing, drawing, gesture or behaviour.
3. Do not promise confidentiality. Explain that information may need to be shared to keep the learner or others safe.
4. Do not ask to repeatedly view, open, forward or save sexual or illegal content. Do not print or copy images.
5. Record what was reported, seen or heard, including date, time, people involved, device/app/platform if known, immediate action and who was informed.
6. Report to the DSL immediately. If the DSL is unavailable and risk may be present, follow the safeguarding escalation route.
7. The DSL will consider referral to the placing school DSL, local authority safeguarding route, police, LADO, Prevent/Channel route, adult safeguarding route where relevant, or specialist reporting routes.

18. Specific online risks

Staff should be alert to, and report, online risks including but not limited to:

- cyberbullying and prejudice-based online abuse;
- grooming, coercion, exploitation and unsafe online contact;
- child sexual exploitation and child criminal exploitation facilitated online;
- harmful sexual behaviour, sexual harassment and sexual violence online;
- nude or semi-nude image sharing and image-based abuse;
- online threats, humiliation, intimidation, blackmail or extortion;
- exposure to pornography, violent, hateful, extremist, self-harm, suicide or eating-disorder content;
- radicalisation, extremist material and conspiracy content that may increase risk;
- scams, financial exploitation, impersonation or identity misuse;
- location sharing, live streaming or contact with unknown adults;
- misuse of AI, deepfakes, manipulated images, voice cloning or impersonation;
- data breaches, lost devices, account compromise or unauthorised access.

19. Data protection, confidentiality and records

- Online safety records will be factual, dated, attributable and stored securely with restricted access.
- Safeguarding records will be stored separately from general learner records and cross-referenced where relevant.

- Data breaches, lost devices, misdirected emails, unauthorised access or accidental disclosure must be reported immediately to the Data Protection Lead/leadership team.
- Sensitive information must only be shared where there is a clear need to know, in line with safeguarding and data protection expectations.
- Retention, transfer and deletion of records will follow the Data Protection Policy, Data Retention Schedule, safeguarding requirements and commissioner/placing school arrangements.

20. Training and learner education

- Staff will receive online safety induction before working unsupervised with learners.
- Staff training will include filtering and monitoring responsibilities, reporting routes, SEND-specific online vulnerability, images and consent, professional boundaries, social media, cyber security, data protection, AI risks and online safeguarding concerns.
- Refresher training will be completed at least annually, or sooner where risk, systems, law, guidance or operational arrangements change.
- Learners will receive accessible online safety teaching matched to their age, developmental stage, communication profile, EHCP outcomes and risk assessment.
- Online safety teaching may include privacy, consent, safe help-seeking, trusted adults, safe communication, image sharing, cyberbullying, scams, online kindness, digital footprints and what to do when something feels wrong.

21. Monitoring and review

This policy will be reviewed annually and sooner where risk, law, guidance, technology or operational arrangements change.

An early review must take place after any significant online safety incident, filtering/monitoring failure, harmful content exposure, data breach, image-sharing concern, allegation or low-level concern involving digital conduct, remote learning concern, new venue, new platform, new device model, new commissioner arrangement, or significant change in learner risk profile.

22. Linked policies and templates

- Safeguarding, Child Protection and Safer Recruitment Policy
- Staff Code of Conduct and Safer Working Practice Policy
- Managing Allegations and Low-Level Concerns Policy
- Data Protection Policy and Privacy Notice
- Data Retention Schedule
- Behaviour Support Policy
- Attendance and Absence Policy
- Risk Assessment Policy
- Lone Working Policy
- Educational Visits and Community Learning Policy

- Whistleblowing Policy
- Complaints Policy
- Acceptable Use Agreement
- Approved Systems Register
- Filtering and Monitoring Review Record
- Online Safety Incident Record
- Image and Media Consent Form

Appendix A: Pre-start online safety completion checklist

Item	Evidence required	Status	Owner/date
DSL/Online Safety Lead named	Name, contact and availability recorded	TO DO	
Deputy DSL named	Name, contact and escalation route recorded	TO DO	
Approved Systems Register complete	Devices, apps, platforms and accounts listed	TO DO	
Filtering arrangements confirmed	For each device, network, venue and platform	TO DO	
Monitoring arrangements confirmed	Who receives/checks alerts and how concerns reach DSL	TO DO	
Venue/community internet assessed	Assurance or decision not to use venue Wi-Fi	TO DO	
Device security controls active	Passwords, MFA, updates, lock screens, secure storage	TO DO	
Image/video process confirmed	Consent, storage, retention and publicity checks	TO DO	
Communication routes agreed	Parents/carers, schools, commissioners, professionals	TO DO	
Remote learning decision made	Approved or not used; if used, risk assessment complete	TO DO	
Staff induction complete	Policy, reporting, filtering/monitoring and conduct covered	TO DO	

Appendix B: Approved systems register

System/ device/app	Purpose	Owner/admin	Users	Data held	Filtering/ monitoring	Review date

Appendix C: Filtering and monitoring review record

Review prompt	Questions to answer	Outcome/action	Owner/date
Before first use	Is filtering and monitoring appropriate for this learner/activity/device/venue?		
Annual review	Are systems still suitable and proportionate?		
After incident	Did filtering, monitoring, supervision or reporting fail or need strengthening?		
New venue/network	Has the internet route been assessed and approved?		
New device/platform	Has it been added to the Approved Systems Register?		
Learner risk change	Do supervision, access or restrictions need changing?		

Appendix D: Online safety incident record fields

- Learner name and date of birth;
- date, time and location of concern;
- staff member recording the concern;
- device, app, platform, website, account or communication route involved, if known;
- what was seen, heard, disclosed or reported;
- learner's own words or communication where possible;

immediate safety actions taken;

- whether any evidence was preserved and how, without copying/forwarding illegal or sexual content;
- who was informed: DSL, Deputy DSL, parent/carer, placing school, commissioner, social care, police, LADO, Prevent/Channel, adult safeguarding;
- decision, rationale, follow-up actions and review date;
- links to safeguarding chronology, behaviour/risk assessment, attendance, allegation/low-level concern or data breach records where relevant.

Appendix E: Accessible acceptable use summary

This summary should be adapted into an accessible format for each learner, using visuals, symbols, social narrative, AAC, easy-read wording or supported practice as needed.

- I use technology for the agreed activity.
- I ask for help if something worries me, upsets me or feels wrong.
- I do not share my personal information with people I do not know.
- I do not take photos, videos or recordings of people unless staff say it is agreed.
- I tell a trusted adult if someone asks me for pictures, secrets, money, my location or to meet up.
- I use kind words online and tell staff if someone is unkind to me.
- Staff will help me learn how to stay safe online.