

NEO — Online Safety and Acceptable Use Policy

26 Aug 2026, 12 min read

NEO by Nudge Education · Version v08.26 · Approved August 2026 ·
Review August 2027

This policy applies to all learners, staff, practitioners, contractors, volunteers and visitors of Nudge Education Online (NEO). NEO is a fully online alternative provision for learners aged 11–18, operated by **Nudge Education Ltd** (Company Number 10192753). NEO is not a DfE-registered independent school and is not subject to Independent Schools Inspectorate (ISI) inspection. NEO is pursuing **OEAS accreditation** only.

1. Policy statement and purpose

NEO is committed to ensuring that children and young people are kept safe when accessing education online. As a fully online alternative provision, digital safety is not a supplementary concern — it is fundamental to every aspect of NEO's safeguarding culture and practice.

This policy sets out how NEO:

- Safeguards learners across all online environments used for teaching, learning, and communication.
- Ensures platforms are used safely, responsibly, and securely by all members of the NEO community.
- Trains staff to identify, manage, and respond to online risks effectively.
- Responds to online safety concerns, cyber incidents, or misuse.
- Embeds responsible, transparent, and consent-gated use of artificial intelligence within its operations, aligned with NEO's agentic-AI design principles.
- Complies with the **Online Safety Act 2023** and the **ICO Children's Code**, and is delivered with regard to **Keeping Children Safe in Education 2026** (in force 1 September 2026), including its online safety and filtering and monitoring expectations.

2. Scope

This policy applies to:

- All learners aged 11–18 enrolled at NEO.
- All staff, practitioners, qualified teachers, contractors, and volunteers.
- All online and digital learning activity, including live lessons, asynchronous work, and communication.
- All platforms and tools used for teaching, communication, safeguarding, administration, and assessment.
- All devices used to access NEO platforms, whether NEO-issued or personal.

3. Approved platforms

NEO uses a restricted, approved set of platforms. The use of unapproved platforms for learner contact is **not permitted under any circumstances**.

3.1 Core teaching and communication platforms

Platform	Purpose	Safeguarding controls
Google Classroom	Curriculum delivery, assignments, resources, feedback, and class communication	Role-based access; managed accounts; assignment privacy settings; guardian summaries
Google Meet	Live online teaching, tutorials, pastoral sessions, and meetings	Host controls; waiting rooms; chat moderation; recording controls; screen-share permissions
Google Workspace	Official communication, document collaboration,	Encrypted at rest and in transit; managed

Platform	Purpose	Safeguarding controls
(Gmail, Drive, Docs, Sheets, Forms)	safeguarding records, registers, and administration	accounts; access controls; audit logs; data loss prevention

3.2 Communication channels

- NEO-managed email accounts are the primary channel for learner–staff communication. All emails are monitored, filtered, and logged.
- Telephone contact (staff only) is used for safeguarding or welfare purposes. Personal phone numbers are never used; all calls are logged.
- No external social media, messaging applications, or community chat platforms (for example Discord, WhatsApp, Instagram DMs) are used for learner communication unless expressly authorised by the DSL and configured to meet NEO safeguarding standards.

3.3 Assessment, administration, and payment systems

- Secure cloud storage for safeguarding records and EHCP evidence.
- Online examination platforms where applicable, subject to DPIA.
- Payment and commissioning systems for invoicing and reporting, with access restricted to the NEO finance function.

This policy applies to all use of the above platforms, whether during teaching, preparation, recording, or communication.

4. Roles and responsibilities

4.1 The Proprietor

- Ensures appropriate policies, oversight, and resourcing for online safety across NEO.
- Receives anonymised reports of online safety incidents and audit outcomes.
- Ensures NEO meets relevant OEAS accreditation criteria relating to online safety and welfare.

4.2 Director, NEO & Head of School

- Operational ownership of online safety arrangements; co-signs this policy with the DSL.
- Ensures adequate investment in filtering, monitoring, and training.
- Holds the Data Protection Officer function during the initial period.

4.3 Designated Safeguarding Lead (DSL)

The DSL holds lead responsibility for online safety and safeguarding. The DSL:

- Responds to online safety concerns involving learners.
- Liaises with local authorities, commissioners, Ofcom (under the Online Safety Act 2023 where applicable), and external agencies.
- Oversees staff training and induction relating to online safety.
- Reviews filtering and monitoring systems termly.
- Coordinates communication during serious incidents.
- Ensures NEO's approach to AI use remains safe, consent-gated, and compliant.

4.4 Cyber security and platform incidents

Operational responsibility for responding to cyber-attacks, data breaches, or platform failures sits with the Director / Head of School, in consultation with:

- The DSL, where there is a safeguarding risk to learners.
- The Data Protection Officer (DPO), for data breaches or UK GDPR implications.
- Platform providers, where their support or disclosure is required.

All incidents are logged, risk-assessed, and escalated appropriately.

4.5 Staff, practitioners, and teachers

All staff must:

- Follow the Acceptable Use Agreement (see Appendix A).
- Use only approved platforms for all learner-facing activity.
- Report online safety concerns immediately to the DSL.
- Maintain professional boundaries in all digital interactions with learners and families.

- Never engage in private, unsupervised digital contact with learners.

4.6 Learners and parents/carers

- Learners are supported to use platforms safely and appropriately through induction and ongoing RSHE with their named practitioner.
- Parents and carers are informed of expectations and responsibilities at induction, and are provided with the **NEO Digital Consent and AI Safety Parent Guide** to support their child's online safety at home.

5. Platform safety, security, and quality assurance

NEO undertakes proportionate due diligence to ensure all platforms are safe and appropriate for use with young people aged 11–18. This includes:

- Use of reputable, education-grade platforms with appropriate safeguarding features.
- Confirmation that data is encrypted in transit and at rest.
- Review of privacy notices, data processing agreements, and security documentation.
- Role-based access controls and permission settings.
- Regular review of platform safeguarding features, updates, and known vulnerabilities.
- Data Protection Impact Assessments (DPIAs) for new or changed platforms.
- Alignment with Ofcom's illegal content risk assessment expectations under the Online Safety Act 2023, where NEO's services fall within scope.

5.1 Access and accounts

- All learners are issued with NEO-managed accounts for accessing Google Classroom, Google Meet, and Google Workspace.
- Personal accounts must never be used for teaching, learning, or safeguarding communication.
- Accounts are deactivated promptly when a learner or staff member leaves NEO.
- Two-factor authentication is required for all staff, practitioner, and teacher accounts.

6. Monitoring and oversight

- All live lessons are supervised and moderated by staff. Session recordings may be reviewed for safeguarding and quality assurance purposes.
- Platform features such as chat, breakout rooms, and permissions are configured proportionately to balance safeguarding with learner agency.
- Concerns arising from platform use are recorded on the NEO safeguarding log and reviewed by the DSL.
- Patterns of concern are analysed termly and used to inform training, platform settings, or policy review.
- All monitoring complies with UK GDPR and the ICO Children's Code, is proportionate, and is carried out in the best interests of learners.

7. Filtering and monitoring standards (KCSIE 2026)

This section applies the filtering and monitoring expectations of **Keeping Children Safe in Education 2026** (in force 1 September 2026) and the DfE filtering and monitoring standards for schools and colleges, adapted for a fully online alternative provision in which learners access education on NEO-managed accounts and enrolled devices rather than on a school premises network. NEO's filtering and monitoring are provided through **Smoothwall**, deployed across NEO-managed accounts and enrolled devices.

In line with KCSIE 2026:

- The **Director, NEO & Head of School is the senior leader responsible for filtering and monitoring**. The DSL takes lead responsibility for understanding the filtering and monitoring systems in place as part of their safeguarding role, and IT support provides technical operation.
- A **review of the effectiveness of filtering and monitoring is carried out at least once every academic year**, led by the senior leader responsible, with the support of the DSL and IT support. The outcome is recorded and reported to the Proprietor.
- The review includes **checks that filtering is working appropriately on all relevant learner accounts and enrolled devices**, and a record is kept of these checks.
- Filtering is appropriate to the age range of learners (11–18), blocks harmful and inappropriate content without unreasonably impacting

teaching and learning, and over-blocking is reviewed so it does not impede legitimate learning.

- Monitoring systems are proportionate and compliant with UK GDPR and the ICO Children's Code.
- **Alert triage.** Smoothwall alerts are triaged first by a designated first-line technical triage lead. Any alert with safeguarding significance is escalated immediately to the DSL, who makes all safeguarding judgements and is the public-facing contact for online safety concerns.
- **Device packages.** Learners on NEO's standard package use managed devices with full Smoothwall filtering and monitoring. For learners on flexible bring-your-own-device packages, filtering and monitoring apply at the level of the NEO-managed account; the differences in coverage on personally owned devices are risk-assessed for each learner on admission and recorded, with additional safeguards agreed with families where needed.
- Smoothwall's monitoring processing is covered by a data processing agreement and a Data Protection Impact Assessment (see the Data Protection and Information Security Policy).
- All staff understand what is filtered and monitored, their role in reporting concerns, and how to escalate concerns about the effectiveness of these systems to the DSL.
- **Generative AI is within scope:** filtering and monitoring arrangements cover learner access to generative AI tools on NEO-managed accounts and devices, in line with KCSIE 2026 and the NEO Artificial Intelligence Policy.
- The Proprietor receives termly assurance that filtering and monitoring standards are being met, in addition to the annual effectiveness review.

8. Training and awareness

8.1 DSL training responsibilities

- Staff receive annual safeguarding and online safety training.
- Updates are provided promptly in response to emerging risks, incidents, or changes in statutory guidance.
- Induction training includes platform-specific safeguarding guidance.

8.2 Staff training

All staff, practitioners, and qualified teachers receive:

- Online safety training at induction.
- Annual refresher training covering safeguarding in online environments, professional boundaries and digital conduct, platform-specific features and risks, AI safety, and responding to online disclosures or incidents.
- Additional training when new platforms or tools (including AI tools) are introduced.

8.3 Learner and parent awareness

- Learners receive online safety education through induction and ongoing RSHE, covering the four areas of online risk: **content, contact, conduct, and commerce**.
- Parents and carers receive guidance through the **NEO Digital Consent and AI Safety Parent Guide** on supporting their child's online safety, recognising risks, and knowing how to report concerns.

9. Responding to online safety concerns

Online safety concerns may include:

- Inappropriate online behaviour by learners or staff.
- Exposure to harmful, illegal, or age-inappropriate content.
- Cyberbullying, online harassment, or child-on-child abuse.
- Misuse of platforms, including unauthorised sharing of session content.
- Sharing of nudes or semi-nudes.
- Grooming, sextortion, or exploitation.
- Data security concerns or breaches of confidentiality.
- AI-related harms, including deepfakes and misinformation targeting learners.

All concerns are reported immediately to the DSL, recorded factually on the safeguarding log, escalated according to safeguarding thresholds, and shared with commissioning schools or local authorities where required.

10. Cyber incidents and data breaches

In the event of a cyber-attack or data breach:

- Immediate steps are taken to secure systems and limit further exposure.
- The DSL and DPO are informed without delay.
- Risks to learners are assessed and safeguarding actions are taken as needed.
- Notifications are made to the ICO within 72 hours and to affected parties in line with data protection law.
- Lessons learned are documented and used to inform system improvements.

11. Responsible use of Artificial Intelligence

NEO permits limited, ethical use of AI tools where they support accessibility, learning, or workload reduction. AI use is governed by NEO's **agentic-AI design principles**: identity containment, consent gates, bounded autonomy, and a human decision-maker in the loop for all decisions that materially affect a learner.

The following principles govern all AI use within NEO:

- AI tools must not replace professional judgement in safeguarding, assessment, or pastoral decisions.
- AI must not be used to process personal data without explicit approval from the DPO and a completed DPIA.
- AI must not be used to analyse learner behaviour, generate safeguarding decisions, or replace relational judgement.
- All AI tools used within NEO must be transparent, explainable, and reviewed by the Director / Head of School and DSL.
- Learners are educated about AI literacy, including how AI-generated content works, its limitations, and the risks of AI-generated imagery, deepfakes, and misinformation.
- Staff must declare when AI has been used in the creation of educational materials, communications, or reports.
- Where AI agents are used in NEO operations, they operate under documented policy contracts and do not act in ways that materially affect a learner without a human decision-maker in the loop.
- All AI use is overseen by the Director / Head of School and the DSL and must be aligned with data protection, safeguarding, and NEO's relational pedagogy.

See also: **NEO Artificial Intelligence Policy (Diamond Standard)**.

12. Monitoring and review

This policy is reviewed annually or sooner if statutory guidance changes.

Termly audits consider online safety incidents, platform use, training uptake, and filtering and monitoring effectiveness. Updates reflect changes in statutory guidance (including Ofcom guidance under the Online Safety Act 2023), emerging technology risks, and feedback from staff, learners, and families. The Proprietor receives at least one substantive online safety report per year.

Appendix A — Acceptable Use Agreement (summary)

All staff, practitioners, teachers, and learners agree to the following when using NEO platforms:

- Use only approved platforms for all NEO-related communication and activity.
- Communicate respectfully and professionally at all times.
- Never share personal contact details, passwords, or account credentials.
- Never record, screenshot, or distribute session content without explicit permission.
- Report any online safety concerns, incidents, or suspicious activity immediately.
- Comply with all safeguarding, behaviour, and data protection expectations.
- Never use NEO platforms to access, create, or share harmful, illegal, or inappropriate content.
- Understand that all activity on NEO platforms may be monitored for safeguarding purposes, in line with UK GDPR and the ICO Children's Code.

A full Acceptable Use Agreement is issued and signed at induction by all staff and learners. Parents and carers are provided with a copy and asked to acknowledge receipt.

Related policies

This policy should be read alongside:

- **NEO Child Protection and Safeguarding Policy**
- **NEO Online Anti-Bullying Strategy**
- **NEO Behaviour and Regulation Policy**
- **Data Protection, Confidentiality and Privacy Policy**
- **SEND Policy**
- **Equality, Diversity and Inclusion Policy**
- **Admissions Policy**
- **Complaints Procedure**
- **NEO Teaching and Learning Policy**
- **NEO Digital Consent and AI Safety Parent Guide**
- **Staff Code of Conduct**

Document control

Field	Value
Version	v08.26
Approved	August 2026
Next Review	August 2027
Owner	Director, Nudge Education Online & Head of School
Policy Owner	Designated Safeguarding Lead (DSL), countersigned by Director, NEO & Head of School
Approver	Proprietor
Operating Company	Nudge Education Ltd (Company Number 10192753)
Accreditation Route	Online Education Accreditation Scheme (OEAS) — accreditation in progress

