Progress Community
By Progress Schools

Health and Safety Policy

2025/2026

Policy issue and updates

Pages	Issue number	Date
New policy	1	December 2025

The following policy has been approved by the CEO, COO, and Governing Board of Directors.

The policy will be reviewed on an annuals basis unless circumstances arise requiring the policy to be reviewed earlier.

Approved by CEO: December 2025

Board signatory: 

Planned Review: August 2026

1. Policy Overview

1.1 The organisation attaches great importance to the health, safety and welfare of staff, students and others engaged in its online activities, and will manage foreseeable risks arising from remote education, digital operations and associated work activities so far as is reasonably practicable, in line with the Health and Safety at Work etc. Act 1974, the Management of Health and Safety at Work Regulations 1999 and relevant education guidance. Provision is delivered primarily through Cypher Learning as the Learning Management System (LMS), Vedamo as the Virtual Learning Environment (VLE) for live sessions, Century Tech for self-paced learning and extra work, Cloud+ for safeguarding oversight during teaching, CPOMS for safeguarding and wellbeing reporting, and Arbor for student information management.

1.2 To achieve this, the organisation will:

- Ensure staff, students and others are not exposed to avoidable risks arising from online sessions, platforms, home working, data use and online engagement, taking account of the Online Education Standards for health, safety and safeguarding.
- Carry out suitable and sufficient risk assessments for online delivery, including platform security, display screen equipment (DSE), lone and remote working, digital safeguarding, behaviour risks, cyber security and data protection.
- Establish clear online procedures covering incident reporting, emergency response in virtual sessions, cyber-security alerts, platform interruptions, behaviour incidents, illness during online delivery, and management of external guests in Vedamo or other approved platforms, with concerns recorded on CPOMS and monitored via Cloud+ where appropriate.
- Provide and maintain safe systems of work for remote contexts, including guidance for home workstation set-up, breaks, reasonable adjustments, and safe use of Cypher Learning, Vedamo, Century Tech, Cloud+, CPOMS and Arbor.
- Provide appropriate information, instruction, supervision and training for safe online practice, incident escalation and safeguarding, ensuring staff understand their responsibilities in line with Keeping Children Safe in Education 2025.
- Consult staff and students on online health and safety matters and keep records of training, incidents and assessments within secure digital systems.

2. Online learning environments

2.1 This Health and Safety Policy has been extended to address the risks associated with delivering education online, including pupils' home learning environments and staff working remotely, as required by the Online Education Standards. The policy applies to full-time online programmes, blended provision and contingency remote education where learners or staff access Cypher Learning, Vedamo, Century Tech or Arbor from home or other non-school locations.

2.2 We maintain a written risk assessment for online delivery that covers home learning environments, workstation set-up, supervision expectations for younger pupils, staff lone-working and use of devices. This is reviewed at least annually and whenever there are significant changes to platforms or ways of working, including major updates or changes in how Cypher Learning, Vedamo, Century Tech, Cloud+, CPOMS or Arbor are used.

2.3 Our business continuity arrangements for online delivery, including response to platform failure and cyber incidents, are set out in the Safeguarding and Business Continuity sections and are reviewed alongside health and safety risk assessments. These arrangements include alternative communication channels, fall-back learning approaches and safeguarding oversight to ensure continuity of education and welfare where primary platforms are unavailable.

3. Organisational responsibilities

3.1 Leaders will ensure health and safety management systems are established, implemented and reviewed for online delivery, but safe practice relies on the cooperation of all staff and learners in virtual environments, including adherence to session protocols, privacy and security controls. All staff receive the Health and Safety Policy and Organisational Arrangements for online delivery; briefings are provided at induction, when the online risk assessment is updated and when new systems or features are introduced on Cypher Learning, Vedamo, Century Tech, Cloud+, CPOMS or Arbor.

3.2 The Chief Operating Officer (COO) (or equivalent accountable officer) and Proprietor hold ultimate responsibility for online health and safety performance, ensuring the policy reflects digital operations, effective monitoring/reporting and periodic audit of online safety controls and incidents, including cyber-related issues. The COO and Directors ensure the Health and Safety Management System is implemented, oversee safer recruitment and safeguarding, implement online risk assessment programmes (DSE, lone working, virtual session risks) and maintain access to competent advice, reporting progress to the Divisional CEO.

3.3 The Health & Safety Manager (Head of Community) coordinates implementation across virtual settings, maintains health and safety documents, develops online risk assessments and safe systems of work, supports digital accident/incident reporting and investigations (including where RIDDOR may apply for work-related injuries during home working), arranges training, identifies safety issues and conducts remote audits and reviews. Operational leads implement the policy in their online provision, allocate mentors and supervise new staff, complete online risk assessments for their areas, ensure staff training on use of Cypher Learning, Vedamo, Century Tech, Cloud+, CPOMS and Arbor, enforce platform protocols and ensure incident reporting and investigation.

3.4 Staff must comply with online health and safety policies and risk assessments; take reasonable care; cooperate with leaders; report hazards (e.g. platform vulnerabilities, phishing, cyberbullying), accidents, near misses, behaviour incidents and safeguarding concerns via CPOMS and designated channels; use equipment and platforms safely; and set a good example in virtual conduct. Learners must follow instructions and online risk controls set by staff, adhere to virtual classroom rules on Vedamo, Cypher Learning and Century Tech, and report concerns and incidents promptly to staff.

3.5 External visitors joining online sessions must be pre-approved, identifiable within the platform, provided with digital visitor information (session etiquette, safeguarding boundaries) and always supervised; access permissions are time-limited and controlled. Contractors providing digital services must comply with relevant health and safety and data security legislation, provide appropriate risk information where changes may affect safety or privacy, and complete inductions aligned to digital environments.

4. Online systems and platforms

4.1 Cypher Learning is used to host course content, assignments, resources and communication channels. Vedamo is the primary platform for live teaching, tutorials and virtual classrooms, including use of waiting rooms, authenticated access and breakout rooms. Century Tech is used for self-paced learning and interventions, with staff monitoring engagement for signs of difficulty or disengagement that may indicate welfare concerns. All external systems confirm alignment with statutory guidance including ‘Generative AI: product safety standards’.

4.2 Cloud+ supports safeguarding oversight and monitoring in line with filtering and monitoring expectations under KCSIE 2025, providing alerts for potential risks during online activity. CPOMS is the secure system for recording, storing and managing safeguarding and wellbeing concerns. Arbor is the secure system for recording behaviour and attendance. All support statutory expectations for record-keeping and information sharing.

5. Key organisational arrangements

5.1 Accident reporting and investigation: All accidents, injuries, near misses and behaviour incidents during work or study time, including within online sessions or home working, must be reported immediately to the relevant manager and recorded in the digital incident system and/or CPOMS as appropriate.

5.2 Child protection and online safety: The Safeguarding and Child Protection Policy and Online Safety arrangements apply fully online, with staff expected to recognise and respond to indicators of abuse, neglect and online harm in remote contexts in line with KCSIE 2025 and the Online Education Standards.

5.3 Display screen equipment (DSE): All DSE users' complete self-assessments for home workstations; guidance covers ergonomic set-up, breaks and screen time, consistent with HSE advice.

5.4 Lone working: Lone working includes staff facilitating or preparing for online sessions without close supervision; a lone-working risk assessment and procedures (check-in/out, escalation contacts, emergency guidance) must be followed. See 'Lone working policy' for more detail.

5.5 Online behaviour: Staff receive training in de-escalation and managing online hostility; incidents (e.g. abusive chat, threats) must be reported and managed in line with Participation Policy and relevant DfE guidance.

5.6 Work-related stress and wellbeing: The organisation applies HSE Management Standards, recognising online-specific stressors such as isolation, high screen time and digital overload, and acts promptly where risks are identified.

6. Online session safety protocols

6.1 Session set-up must ensure waiting rooms or lobbies are used, authenticated access is enabled, and recording settings are configured in line with policy; Cloud+ monitoring is used where appropriate to support safeguarding and filtering/monitoring duties. Staff verify learner identity, record attendance, respond to absence or disengagement in line with attendance and safeguarding procedures, and log any concerns arising in-session on CPOMS.

6.2 If a participant appears unwell or unsafe, staff pause or terminate the session for that learner, attempt contact via approved channels, engage emergency contacts and call emergency services with the recorded address where there is immediate risk, recording actions on CPOMS. External guests are pre-approved, briefed on safeguarding and conduct, supervised throughout, and removed and reported if expectations are breached.

7. Data protection, business continuity and review

7.1 All use of Cypher Learning, Vedamo, Century Tech, Cloud+, CPOMS and Arbor must comply with UK GDPR and the Data Protection Act 2018, including secure access control, data minimisation and appropriate retention and deletion of records. Our business continuity arrangements for online delivery, including response to platform failure and cyber incidents, are set out in the Safeguarding and Business Continuity plan and are reviewed alongside health and safety risk assessments, reflecting DfE expectations for resilient online provision.

7.2 Health and safety, safeguarding and online safety records relating to online delivery (including risk assessments, training logs, incident reports, audits and action plans) are maintained securely and reviewed at least annually or after significant change, with findings reported to governance.

8. Related policies

8.1 All students, parents/carers and staff should also read the related policies for specific additional information.

- Lone worker policy
- Online safety policy
- Code of conduct
- Risk assessment policy