



ACHIEVE INSPIRE and MOTIVATE CIC
(AIM CIC)

Online Safety Policy

The policy is provided to all AIM CIC Members and Associates at induction alongside our Code of Conduct.

This policy will be reviewed in full by the Board of Directors on an annual basis. This policy was last reviewed and agreed by the Board on 24th July 2026 It is due for review on 24th July 2027.

A handwritten signature in black ink, appearing to read 'J. G. Smith', written over a horizontal line.

Signature

24th July 2026

(Operations Director/Safeguarding Officer)

The minutes of the AIM CIC Board decision made at a Virtual Board meeting on 24th July 2026 clearly demonstrate where this Policy has been developed with the staffing group using their expertise and knowledge.

Publication date: 24th July 2026

Renewal Date: 24th July 2026

Online Safety Policy

Organisation: [Achieve Inspire & Motivate CIC](#). Applies to: All staff, volunteers, contractors, learners, and visitors Approved by: [Dean Goodwin – Director](#). Effective from: [24/07/2026](#) Review cycle: [Annual](#)

1) Purpose and Scope

- The purpose of this policy is to ensure a safe, respectful, and legally compliant online learning environment across all ICT-enabled lessons and activities.
- This policy covers the use of devices, networks, internet services, learning platforms, cloud apps, and digital communications used for teaching, learning, assessment, and administration, whether on-site or remote.

2) Our Commitment

- We are committed to safeguarding children, young people, and adults at risk online and offline, and to protecting everyone's privacy and dignity.
- We will comply with applicable laws and guidance on safeguarding, data protection, intellectual property, and acceptable internet use.
- We will foster a culture where unsafe or inappropriate online behaviour is challenged, and concerns can be raised without fear of retaliation.

3) Roles and Responsibilities

- Board/Directors: Set expectations, allocate resources, approve and review this policy, and receive safeguarding and online-safety reports.
- Designated Safeguarding Lead (DSL): [Dean Goodwin – Director](#). Leads on online-safety safeguarding issues, coordinates responses, and maintains records.
- Data Protection Lead (DPL): [Jon Phipps – Director](#). Oversees data protection compliance, DPIAs, and breach response.
- ICT Lead/Provider: [External](#). Manages technical controls, filtering, device configuration, updates, and monitoring in line with this policy.
- Staff and Volunteers: Model safe behaviour, use approved systems, follow this policy in all ICT-enabled lessons, and report concerns promptly.
- Learners: Follow the Learner Acceptable Use Agreement, protect personal information, treat others respectfully, and report concerns.
- Parents/Carers (where applicable): Support safe use at home and review the Learner Acceptable Use Agreement with the learner.

4) Acceptable Use Standards

- Use only CIC-approved accounts, devices, and platforms for teaching, learning, and communications.

- Keep logins private; use strong passwords and multi-factor authentication where provided.
- Access only age and role appropriate content and resources. Do not attempt to bypass filtering or security controls.
- Prohibit bullying, harassment, hate speech, discrimination, sexualized content, extremist content, and illegal sharing.
- Follow copyright and licensing rules; credit sources.
- No recording, photographing, or sharing of lessons or individuals without consent and a legitimate purpose.

5) Safeguarding in ICT-Enabled Lessons

- Planning: Select age-appropriate tools and content; consider accessibility and diverse needs.
- Delivery:
 - At the start of each course/module, set class norms for online conduct and privacy.
 - Use waiting rooms, mute, chat controls, and screen-share limits in live sessions.
 - For remote lessons, avoid one-to-one unsupervised video. If needed, obtain prior approval, log the session, and use CIC accounts.
- Content and Contact Risks: Integrate age-appropriate digital citizenship (privacy, misinformation, respectful communication, reporting).
- Reporting: Learners and staff can report concerns to the DSL via [email/phone/form]. Concerns about immediate risk are escalated the same day.

6) Technical and Organisational Controls

- Secure Devices: Company devices are encrypted, auto-lock after inactivity, and run up-to-date OS/patches and anti-malware.
- Network and Filtering: On-site networks use content filtering and safe search where feasible. For remote learning, learners receive guidance on home filtering/parental controls.
- Access Management: Role-based access; least-privilege permissions for staff and learners; prompt revocation on role change or exit.
- Backups and Continuity: Curriculum and learner records stored in approved systems with regular backups and recovery testing.
- Approved Platforms: Maintain a register of approved teaching platforms and apps. Conduct a lightweight DPIA for new tools before use.

- Data Minimization: Collect only what is necessary; use privacy settings that default to minimal data sharing.

For examples of practical security measures (e.g., updates, backups, access control), see typical regulatory guidance. autoriteitpersoonsgegevens.nl.

7) Data Protection and Privacy

- Lawful Basis: Define lawful bases for processing learner and parent data; provide a clear privacy notice.
- Special Category Data: Store and share safeguarding and health information on a strict need-to-know basis with enhanced security.
- Data Sharing: Share externally only where lawful and necessary (e.g., with schools, social services, exam bodies), recording the rationale.
- Retention: Follow retention schedules for lesson recordings, chat logs, assessments, and safeguarding records.
- Rights: Honor data subject rights (access, rectification, erasure where applicable); route requests to the DPL.

8) Education, Training, and Communication

- Staff: Induction plus annual refreshers on online safety, safeguarding, and data protection; tool-specific training for new platforms.
- Learners: Regular, age-appropriate sessions on online conduct, privacy, cyberbullying, misinformation, scams, and reporting routes.
- Parents/Carers: Provide concise guides on supporting safe learning at home, device settings, and how to raise concerns.

For general structure in writing and communicating a safety policy, see OSHA's guidance on policy statements and roles. osha.gov.

9) Incident Response and Escalation

- Recognizing Incidents: Inappropriate content, suspected grooming, bullying/harassment, data loss/breach, platform compromise, or illegal content.
- Immediate Actions:
 - Preserve evidence (screenshots, URLs, logs) without sharing further.
 - Remove access to offending content; isolate affected accounts/devices.
 - Report to DSL immediately; for data breaches, notify the DPL; consider external reporting obligations.
- Safeguarding: DSL assesses risk, contacts appropriate agencies if needed, and records actions and outcomes.

- Communication: Inform affected parties as appropriate; avoid naming individuals beyond need-to-know.
- Review: Post-incident review to improve controls, lessons plans, and training.

10) Remote and Hybrid Learning Safeguards

- Use CIC accounts; disable private chat between learners unless moderated.
- Recordings: Record only when pedagogically necessary; announce at start; store securely with retention limits; never publish recordings that identify learners without consent.
- Environment: Encourage neutral or blurred backgrounds; avoid sharing personal contact details; use virtual waiting rooms.

11) E-Safety Topics Embedded in Curriculum

- Respectful online communication and digital footprint.
- Privacy settings, passwords, and phishing awareness.
- Evaluating sources, AI literacy, and misinformation.
- Intellectual property, citation, and fair use.
- Wellbeing: screen time, balance, and help-seeking strategies.
- Environmental awareness of e-waste and sustainability where relevant to ICT topics. padayonfutureteachers.weebly.com.

12) Monitoring, Reporting, and Review

- Monitoring: Proportionate review of platform logs and safeguarding reports by DSL/ICT Lead; no covert surveillance.
- Metrics: Termly summary to Board of incidents, training completion, and any DPIAs or platform changes.
- Review: Annual policy review or sooner after incidents, legal changes, or curriculum shifts. Sign and date updates.

13) Related Documents

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Complaints Policy
- Staff Code of Conduct

14) Policy Ownership and Approval

- Owner: Dean Goodwin – Director
- Approved by: AIM Board of Directors

• Signature: 

Date: 24/07/2026