

Online Safety and Acceptable Use Policy

Document control	Detail
Policy title	Online Safety and Acceptable Use Policy
Version	3.0
Status	Approved for use
Policy owner	Hannah Lewis – Education Lead / DSL
Approved by	Nathan Warr – Operations / Governance Lead
Applies to	Directors, employees, tutors, associate tutors, subcontractors, volunteers and any person working on behalf of PACE Education Pathways
Date approved	21/08/2026
Next review date	12 months from approval, or earlier where a review trigger applies
Review trigger	Earlier review if statutory guidance, technology, platforms, commissioner requirements or the service model changes, or following a serious online-safety incident, safeguarding concern, data breach, complaint or audit finding.
Linked documents	Safeguarding and Child Protection Policy; Data Protection and UK GDPR Policy; Privacy Notice; Staff Code of Conduct and Low-Level Concerns Policy; Managing Allegations Against Staff Policy; Incident Reporting Policy; Prevent, Extremism and Radicalisation Policy; Attendance and Engagement Policy; Parent / Carer Consent and Information Sharing Form; Online / Remote Learning Risk Assessment Template; Data Breach Log; Safeguarding Concern Form

Governance note

Online safety is part of safeguarding. PACE uses technology to support flexible 1:1 provision, but digital delivery must never create secrecy, blurred professional boundaries, unmanaged safeguarding risk or unnecessary exposure of personal data. Where an online concern also engages safeguarding, staff conduct, Prevent, data protection or incident-reporting procedures, the relevant specialist process must be followed immediately.

1. Purpose

This policy establishes safe, lawful and professionally bounded use of technology across PACE provision. It covers online teaching, communication, devices, platforms, images, recordings, social media, artificial intelligence and cyber-security controls, and links online delivery to the PACE Online / Remote Learning Risk Assessment.

2. Scope

This policy applies to staff, tutors, pupils and, where relevant, parents/carers using technology as part of PACE activity. It applies to online tutoring, email, messaging, video calls, shared documents, learning platforms, websites, devices, cloud services, images, social media, AI tools and any digital communication connected to provision.

3. Legal and guidance framework

PACE will apply the current version of relevant law and statutory guidance, including Keeping Children Safe in Education online-safety expectations, Working Together to Safeguard Children, UK GDPR and the Data Protection Act 2018, the Prevent duty where relevant, and commissioner requirements. PACE will also follow its safeguarding, staff conduct, data protection, incident reporting and risk-assessment arrangements.

4. Roles and responsibilities

Role	Responsibilities
Education Lead / DSL	Own safeguarding aspects of online provision; approve or review higher-risk arrangements; respond to digital safeguarding concerns; coordinate commissioner or statutory escalation.
Operations / Governance Lead	Maintain approved systems, data/security controls and assurance arrangements; support breach response, incident review and policy audit.
Staff / tutors	Use approved systems, follow professional boundaries, complete required risk assessments, protect information, record attendance and report concerns promptly.
Parents / carers / commissioners	Provide relevant information, support agreed supervision or emergency arrangements where applicable, and notify PACE of concerns or changes affecting safe online delivery.

5. Acceptable staff use and professional boundaries

- Use approved PACE communication channels and accounts wherever possible.
- Keep all digital contact purposeful, professional and capable of being evidenced.
- Do not use personal social media accounts to contact, follow or privately message pupils.
- Do not share personal contact details with pupils unless specifically authorised, necessary and risk assessed.
- Do not use technology to create secrecy, dependency, favouritism or blurred boundaries.
- Do not store pupil images, safeguarding records or sensitive information on personal devices or personal cloud accounts unless specifically authorised and protected.
- Escalate any boundary-testing, sexualised, threatening, discriminatory or otherwise concerning communication.

6. Online / remote learning risk assessment

Before online or remote learning begins, PACE will complete or confirm a proportionate Online / Remote Learning Risk Assessment for the pupil and delivery arrangement. The assessment should be reviewed when circumstances materially change and after a significant incident or safeguarding concern.

- approved platform and account arrangements;
- pupil age, SEND, communication, behaviour, medical and welfare needs;
- supervision and parent/carers awareness where appropriate;
- privacy of tutor and pupil environments;
- contingency if connection is lost;
- unauthorised access, recording, harmful content, third-party presence and data-sharing risks;

- emergency contacts, safeguarding escalation and circumstances in which a session must be stopped.

7. Standards for online sessions

- Sessions must be planned, purposeful and appropriate to the pupil's age, needs and agreed provision.
- Staff must use a professional background and environment and should avoid private sleeping spaces or settings that could compromise boundaries.
- Only authorised participants should join. Unexpected adults, unidentified participants or inappropriate content may require the session to be paused or ended.
- Recording is prohibited unless there is a clear purpose, lawful basis, prior approval and appropriate information/consent arrangements.
- Staff must not capture informal screenshots, photographs or recordings of pupils.
- Attendance must be recorded in accordance with the Attendance and Engagement Policy and significant concerns recorded through the appropriate safeguarding or incident system.

8. Pupil acceptable use

- Use technology for agreed learning and communication purposes.
- Do not record, photograph or screenshot staff or sessions without permission.
- Do not send or display abusive, sexual, discriminatory, threatening, extremist or otherwise harmful content.
- Do not share passwords or unnecessary personal information.
- Respect reasonable instructions about cameras, microphones, chat, screen sharing and platform use.
- Concerns or breaches will be managed proportionately, taking account of age, SEND, safeguarding and commissioner arrangements.

9. Filtering, monitoring and platform controls

PACE does not operate as a school network provider. Where pupils use school or local-authority devices or networks, the commissioner remains responsible for the filtering and monitoring controls attached to those systems. Where PACE provides or controls a device, account, platform or network, it will apply proportionate access, safe-search, supervision, account and security controls appropriate to the service and risk. A lack of technical filtering does not remove the staff duty to supervise, risk assess and respond to harmful content.

10. Images, recordings and media

- Only create or use pupil images, video or audio where there is a clear educational, safeguarding or operational purpose and a lawful basis.
- Use approved devices and storage arrangements.
- Do not use identifiable pupil material for marketing, publicity or social media without appropriate explicit permission and safeguarding consideration.
- Report accidental capture, receipt or sharing of inappropriate or sensitive material immediately.

11. Artificial intelligence tools

AI may support generic planning, drafting or resource development, but professional judgement remains essential. Staff must not enter identifiable pupil, safeguarding, SEND, health, family or confidential commissioner information

into public or unapproved AI tools. AI-generated material must be checked for accuracy, bias, age-appropriateness, safeguarding risk and copyright or confidentiality concerns before use. AI must not be relied upon to make safeguarding, suitability, disciplinary or other high-impact decisions about a child or staff member.

12. Cyber and data security

- Use strong unique passwords and multi-factor authentication where available.
- Keep devices and software updated and protected.
- Check recipients carefully before sending sensitive information.
- Use secure sharing methods for sensitive or special-category information.
- Avoid public Wi-Fi for sensitive activity unless suitable protection is in place.
- Lock devices when unattended and prevent family members or third parties accessing PACE information.
- Report lost devices, compromised accounts, phishing, malware or suspected unauthorised access immediately.

13. Safeguarding, harmful content and disclosures

Online safeguarding concerns must be treated with the same urgency as concerns arising face to face. Staff must not investigate beyond what is necessary to establish immediate safety. Where a pupil discloses harm, displays concerning material, appears to be at immediate risk, or digital activity suggests exploitation, grooming, sexual harm, bullying, radicalisation, self-harm or another safeguarding issue, staff must follow the Safeguarding and Child Protection Policy and notify the DSL without delay.

14. Data breaches, incidents and session termination

1. Make the situation safe and protect the pupil or other affected person.
2. Pause or end the session where continuing would increase safeguarding, conduct, privacy or security risk.
3. Notify the DSL immediately for safeguarding concerns and the Governance Lead for data/security or serious operational incidents.
4. Record the event using the relevant safeguarding, incident or data-breach process.
5. Notify parents/carers, commissioners, the ICO, police or other agencies where required by the applicable policy or law.
6. Review the risk assessment and controls before provision resumes where a material risk has changed.

15. Training, monitoring and review

Staff must receive online-safety, safeguarding, professional-boundary and data-protection induction appropriate to their role. Training and policy awareness will be recorded through PACE workforce compliance arrangements. The Education Lead / DSL and Governance Lead will review significant online-safety incidents, data breaches, low-level concerns, complaints, safeguarding themes and commissioner feedback to identify trends and required improvements. This policy will be reviewed at least annually and earlier when a review trigger in the document-control table applies.

Appendix A – Online session quick check

Check	Confirmed
Approved platform/account being used	Yes / N/A
Risk assessment current and controls understood	Yes / N/A
Tutor environment professional and private	Yes / N/A
Emergency / safeguarding contacts available	Yes / N/A
Recording or screenshots disabled unless authorised	Yes / N/A
Connection-loss and session-stop contingency understood	Yes / N/A