Cardiff Academy

POLICY /// INFORMATION AND DATA

Online Safety, Acceptable Use, Social Media and Images Policy

Rules and safeguards for the use of Academy IT systems, the internet, personal devices, social media, generative AI and photographs or video, including filtering and monitoring, online risks for students under 18, and consent for images.

REFERENCE	**CA-INF-03**	VERSION	**1.0 (Approved)**
POLICY OWNER	**Designated Safeguarding Lead (with the Head of Operations for IT security)**	APPROVED BY	**Senior Leadership Team (reported to the Board)**
ISSUE DATE	**October 2026**	APPROVAL DATE	**October 2026**
REVIEW CYCLE	**Annual**	NEXT REVIEW DUE	**October 2027**
APPLIES TO	**All students, staff, governors, contractors and visitors using Academy IT or appearing in Academy images**	PUBLISHED	**Website; Student Handbook (acceptable use agreement); staff portal**

RELATED POLICIES CA-WEL-01 Safeguarding and Child Protection; CA-WEL-02 Prevent Duty; CA-INF-01 Data Protection; CA-ACA-05 Academic Integrity and Misconduct; CA-WEL-05 Anti-Bullying, Harassment and Sexual Misconduct; CA-HR-02 Staff Code of Conduct

LEGAL ENTITY Cardiff Education Group Ltd, trading as Cardiff Academy (Company No. 14569122). Registered office: 168 City Road, Cardiff CF24 3JE. Teaching premises: 8 Drake Walk, Cardiff CF10 4LG

1 Purpose

Technology is central to study and university preparation. This policy helps students and staff use it safely, legally and responsibly, protects students – especially those under 18 – from online harm, and protects the Academy's systems and data.

2 Online safety

2.1 Risks we address

The main areas of online risk are **content** (harmful, illegal or extremist material, misinformation), **contact** (grooming, exploitation, radicalisation, fraud), **conduct** (cyberbullying, sharing nude or semi-nude images, plagiarism), and **commerce** (scams, gambling, financial exploitation).

2.2 Filtering and monitoring

- Academy Wi-Fi and devices use web filtering that blocks illegal content, extremist and terrorist material, pornography, gambling and malware.
- Monitoring alerts (for example searches for self-harm or extremist content) are reviewed by the DSL team, who act under CA-WEL-01 or CA-WEL-02.
- The DSL and Head of Operations review the effectiveness of filtering and monitoring at least annually and record the review.
- Students and staff who need to access sensitive material for legitimate study must agree this in advance with the DSL.

2.3 Education

Online safety is covered at induction and through tutorials, including: protecting personal information; recognising scams (including visa and accommodation scams aimed at international students); healthy relationships and consent online; cyberbullying; misinformation and extremism; and responsible use of AI.

3 Acceptable use – students

By using Academy IT, students agree to:

- use their own account only and keep passwords private
- use Academy systems for study and reasonable personal use only
- not access, create, store or share illegal, extremist, pornographic, violent, discriminatory or abusive material
- not bully, harass, threaten or impersonate anyone online
- not attempt to bypass filtering (for example using VPNs or proxies on the Academy network)
- not install unauthorised software, introduce malware, or attempt to access systems or data without permission
- respect copyright and not submit others' work as their own
- use generative AI only as permitted by their teachers and CA-ACA-05
- not record staff or students without permission

Students sign the **Student Acceptable Use Agreement** at enrolment. Breaches are handled under CA-WEL-04 Student Code of Conduct and Disciplinary Policy and, where relevant, CA-WEL-01.

4 Personal devices

Students may use personal devices on the Academy Wi-Fi, subject to this policy. Mobile phones must be silent in lessons and are not allowed in examinations. The Academy is not responsible for loss or damage to personal devices.

5 Acceptable use – staff

Staff must:

- use Academy email and approved platforms for all communication with students; not use personal phone numbers, personal email or personal social media accounts to contact students, except in an emergency with the DSL's agreement
- not accept or send "friend" or "follow" requests to current students (or former students under 18) on personal social media
- protect personal data as set out in CA-INF-01, and never enter student personal data into unapproved AI tools
- report any online safety concern about a student to the DSL immediately
- follow the Staff Code of Conduct (CA-HR-02) in all online activity, including outside work, so as not to bring the Academy into disrepute

6 Online teaching

Live online lessons take place only on Academy-approved platforms using Academy accounts. Staff must not teach one-to-one online with a student under 18 without the DSL's agreement, and sessions with under-18s are recorded or have a second adult present where practicable. Recordings are stored securely and deleted in line with the retention schedule.

7 Social media

- The Academy's official accounts are managed by authorised staff only. Posts follow the brand guidelines and CA-GOV-11.
- Students and staff must not create accounts or groups that claim to represent the Academy without permission.
- Concerns about inappropriate posts involving the Academy should be reported to the Head of Operations; posts involving harm to a student are reported to the DSL.

8 Photographs, video and images

8.1 Consent

- Photographs or video of students are used for publicity (website, prospectus, social media, agent materials) **only with written consent**. For students under 18, consent is obtained from the parent or guardian and the student.
- Consent can be withdrawn at any time; the Academy will stop new use and remove images from its own channels where practicable.

- Consent preferences are recorded on the student record and checked before any image is published.

8.2 Rules

- Only Academy devices are used by staff to take photographs or video of students. Images are transferred to secure Academy storage and deleted from devices promptly.
- Students' full names are not published alongside images of students under 18 without specific consent; addresses and other identifying details are never published.
- Images must be appropriate: students suitably dressed, no images in toilets or changing areas, and nothing that could cause embarrassment or be misused.
- Students must not photograph or film others without their consent, and must never share intimate images of anyone. Sharing nude or semi-nude images of a person under 18 is a criminal offence and a safeguarding matter.
- Visitors (including partner universities and media) may photograph students only with the Academy's agreement and student consent.

9 Reporting concerns

Students can report online concerns to any member of staff, the DSL, or through the Cardiff Academy app. Illegal content involving children can also be reported to the Internet Watch Foundation, and online child sexual abuse to CEOP.

10 Review

This policy is reviewed annually, and whenever there are significant changes in technology, risk or guidance.

Compliance mapping

This policy has been written to meet, and to evidence, the following external requirements. Inspectors and university partners can use this table to locate the relevant provisions.

ISI Educational Oversight (PFE) standards	Standard 40 (safeguarding arrangements including online safety); Standard 16 (resources); Section 4 criteria on radicalisation and extremism (filtering)
British Council Accreditation UK criteria	P9 (educational technology fit for purpose); S1–S2 (safeguarding of under 18s); W3 (procedures for dealing with abusive behaviour)
University partner due diligence	Partner due diligence – IT acceptable use and online safety policy
Legislation and statutory guidance	Keeping Learners Safe (Wales, 2022) and Welsh Government guidance on online safety; Prevent duty guidance (2023) on filtering; Online Safety Act 2023; Computer Misuse Act 1990; UK GDPR; Copyright, Designs and Patents Act 1988; Malicious Communications Act 1988; Protection of Children Act 1978

Document control

Version	Date	Author / reviewer	Summary of changes

1.0	October 2026	Designated Safeguarding Lead (with the Head of Operations for IT security)	New policy written for university partnerships, ISI Educational Oversight and British Council Accreditation UK. Supersedes all previous versions.

APPROVED ON BEHALF OF THE BOARD	SIGNATURE	DATE
Chair of the Board of Governors		