

E-Policy, Social Media and Electronic Devices Policy

Glasgow Maritime Academy LLP (GMA) recognises the educational value of digital technology while maintaining a safe, professional, respectful and effective learning environment.

This policy applies to all participants, staff, lecturers, assessors, contractors and visitors and should be read alongside the relevant Staff and Participant Codes of Conduct.

1. Purpose

This policy sets out acceptable standards for the use of digital technology during Academy activities, including:

- mobile telephones;
- tablets, laptops and computers;
- cameras and recording devices;
- smart watches and other connected devices;
- social media and messaging applications;
- Academy internet and Wi-Fi services;
- online learning and video-conferencing platforms;
- artificial intelligence and other digital learning tools.

It applies to classroom, simulator, workshop, practical, assessment, examination, online, blended and other Academy-related activities.

2. General principles

Technology must be used in a way that:

- supports rather than disrupts learning;
- respects the privacy, dignity and rights of others;
- protects confidential and personal information;
- maintains the security and integrity of examinations and assessments;
- does not compromise health and safety;
- does not involve discrimination, harassment, bullying, cyberbullying or intimidation;
- does not contain false, abusive, threatening, defamatory or unlawful material relating to another participant, member of staff or the Academy;
- complies with applicable law and Academy policies.

3. Mobile telephones, tablets and other devices during training

Participants must place mobile telephones and other personal devices on silent mode during teaching, practical exercises, simulator sessions and assessments unless their use has been authorised by the instructor.

Devices may be used for legitimate course-related purposes where permitted by the instructor. Participants must not use devices in a way that distracts themselves or others from teaching, assessment, safety briefings or practical exercises.

Where an individual has an urgent personal or operational need to remain contactable, this should normally be discussed with the instructor before the session. Reasonable use of technology required as an agreed adjustment will be supported where appropriate.

4. Photography, audio recording and video recording

Participants must not photograph, film, audio-record, live-stream or screen-record any teaching session, practical activity, assessment, simulator exercise, member of staff or other participant without prior permission.

Recording is strictly prohibited where it would:

- capture examination or assessment material;
- compromise examination or assessment security;
- reveal confidential, commercially sensitive or personal information;
- capture another person without appropriate authority or consent;
- interfere with a practical or safety-critical exercise;
- breach copyright, data protection or another legal obligation.

GMA may record teaching or assessment activity for authorised educational, quality, security or evidential purposes. Where this occurs, participants will be informed as appropriate and recordings will be managed in accordance with the Academy's privacy and data-protection arrangements.

5. Social media

Participants and staff are personally responsible for material they publish on social media or digital communication platforms. GMA does not prohibit lawful personal use of social media, but Academy-related use must not:

- contain discriminatory, threatening, abusive, harassing or defamatory material;
- constitute bullying or cyberbullying;
- disclose personal or confidential information without authority;
- publish photographs or recordings of another participant or staff member without appropriate permission;
- disclose examination questions, assessment materials or restricted course content;
- falsely represent an individual's personal opinion as an official GMA statement;
- impersonate another individual or use another person's account;

- infringe copyright or intellectual-property rights;
- compromise the safety, security or welfare of participants or staff.

Concerns about online behaviour that affect the learning environment, welfare of participants or reputation of individuals may be addressed by GMA even where the content was created away from Academy premises.

6. Online and blended learning

Participants attending remotely must comply with the same standards of conduct that apply on Academy premises.

Participants must not:

- give another person access to their personal learning account;
- share restricted meeting links or passwords;
- allow another individual to undertake attendance, training or assessment on their behalf;
- record or redistribute an online class without permission;
- use unauthorised material, websites, software or artificial intelligence during an examination or controlled assessment;
- interfere with another person's participation.

Where identity verification, camera use or other monitoring is required for an assessment, participants will be informed in advance. Personal information collected for this purpose will be handled in accordance with the Academy's privacy arrangements.

7. Artificial intelligence

AI tools may be used for learning where their use is permitted by the lecturer or course arrangements. AI must not be used to:

- complete an assessment intended to demonstrate the participant's own competence;
- generate answers during a closed-book or controlled examination;
- impersonate another person;
- falsify attendance, assessment or evidence;
- process confidential or personal information without authority.

Unauthorised use of AI in an assessment may be treated as assessment misconduct.

8. Academy systems and internet access

Users of GMA networks, devices and systems must not knowingly:

- introduce malware or malicious software;
- attempt to bypass security controls;
- access another person's account or records without authority;
- access, download or distribute illegal or seriously inappropriate material;

- interfere with Academy networks, equipment or data;
- use Academy systems for unlawful activity.

Suspected cybersecurity incidents must be reported promptly to a member of staff.

9. Staff responsibilities

Staff must model appropriate digital behaviour and apply this policy consistently. Particular care must be taken when communicating with participants digitally, storing participant information, photographing or recording participants, publishing Academy material online, using personal devices for Academy business, handling assessment material and using AI systems with participant or Academy information.

10. Breaches of this policy

Minor breaches will normally be addressed promptly by the lecturer or responsible member of staff. Repeated, deliberate or serious breaches may result in proportionate action, including:

- 1 a verbal instruction or warning;
- 2 a formal written warning;
- 3 removal from the affected session;
- 4 restriction of access to Academy systems or facilities;
- 5 investigation under the relevant Code of Conduct;
- 6 removal from a course where justified;
- 7 withholding of certification where course-completion requirements have not been met;
- 8 referral to an appropriate external authority where required.

11. Reporting concerns

Participants should report inappropriate digital conduct, cyberbullying, unauthorised recording, online harassment or misuse of personal information to their lecturer, the Academy administration team or senior management. Reports will be handled sensitively and, as far as reasonably possible, confidentially. No participant will be disadvantaged for raising a genuine concern in good faith.

12. Communication and review

This policy will be made available to participants and staff, referenced during induction and linked to the Staff and Participant Codes of Conduct. Its effectiveness will be monitored through feedback, incident records, complaints, observations and internal review. The policy will be reviewed at least annually and whenever significant changes to legislation, technology or Academy delivery methods require an earlier review.