

Online Safety Policy

Online Safety Policy

Organisation: EMZ AESTHETICS LTD

Effective Date: 1st September 2026

Review Date: 1st September 2027

1. Purpose

The purpose of this Online Safety Policy is to ensure that all learners, staff, contractors, and visitors use digital technologies safely, responsibly, and ethically. This policy aims to protect individuals from online risks while promoting a positive and secure digital learning environment.

2. Scope

This policy applies to:

- All employees and volunteers.
 - All learners.
 - Contractors and visitors using organisation-owned systems or networks.
 - All devices used to access organisational systems, whether organisation-owned or personal.
-

3. Policy Statement

EMZ AESTHETICS LTD is committed to:

- Providing a safe online learning environment.
 - Protecting learners and staff from online abuse, cyberbullying, and inappropriate content.
 - Promoting responsible digital behaviour.
 - Ensuring compliance with data protection legislation.
 - Responding promptly to online safety concerns.
-

4. Acceptable Use

Users must:

- Use technology for educational and professional purposes.
- Treat others respectfully online.
- Protect usernames and passwords.
- Log out of devices when finished.
- Report suspicious emails, messages, or online activity immediately.
- Respect copyright and intellectual property rights.

Users must not:

- Access inappropriate, offensive, or illegal content.
 - Share confidential or personal information without permission.
 - Use another person's account.
 - Download unauthorised software.
 - Engage in cyberbullying, harassment, or discrimination.
 - Use organisational systems for illegal or unethical activities.
-

5. Learner Responsibilities

Learners are expected to:

- Follow this policy at all times.
 - Keep login details secure.
 - Report online safety concerns to a tutor or designated safeguarding lead.
 - Use respectful language during online lessons and communications.
 - Protect their own personal information and the information of others.
-

6. Staff Responsibilities

Staff must:

- Model safe and responsible online behaviour.
- Monitor online learning environments appropriately.
- Report safeguarding concerns immediately.
- Maintain professional boundaries when communicating online.
- Use approved communication platforms.
- Complete online safety and safeguarding training.

7. Cyberbullying

Cyberbullying includes:

- Sending abusive messages.
- Sharing harmful or embarrassing content.
- Threatening or intimidating others online.
- Creating fake accounts.
- Excluding individuals from online groups deliberately.

Any reports of cyberbullying will be investigated promptly and managed in accordance with the organisation's Behaviour, Safeguarding, and Disciplinary Policies.

8. Online Learning

When participating in online learning:

- Learners should attend from an appropriate environment where possible.
 - Appropriate language and behaviour must be maintained.
 - Recording sessions without permission is prohibited.
 - Cameras and microphones should be used in accordance with tutor instructions.
 - Personal information should not be shared during online sessions.
-

9. Data Protection

The organisation will:

- Process personal data in accordance with applicable data protection legislation.
 - Store learner information securely.
 - Limit access to authorised personnel only.
 - Report any data breaches in line with organisational procedures.
-

10. Social Media

Staff and learners should:

- Maintain professional conduct on social media.
 - Avoid sharing confidential organisational information.
 - Report any concerning online interactions involving learners.
 - Follow the organisation's Social Media Policy where applicable.
-

11. Online Safety Incidents

Any concerns involving:

- Cyberbullying
- Online grooming
- Extremist material
- Inappropriate communications
- Data breaches
- Phishing or scams
- Online harassment

must be reported immediately to the Designated Safeguarding Lead (DSL) or line manager.

Where necessary, incidents may be referred to external agencies, including the police or local safeguarding partners.

12. Monitoring

The organisation reserves the right to monitor the use of organisational systems, devices, email, and internet access where lawful and proportionate to protect users, maintain security, and investigate concerns.

13. Training

The organisation will provide regular online safety training for staff and appropriate guidance for learners to ensure awareness of:

- Cyber security
- Phishing awareness
- Password security

- Safe use of AI technologies
 - Data protection
 - Digital wellbeing
 - Online safeguarding
-

14. Breaches of the Policy

Failure to comply with this policy may result in:

- Informal or formal disciplinary action.
 - Removal of access to organisational systems.
 - Referral under safeguarding procedures.
 - Referral to external agencies where appropriate.
-

15. Related Policies

This policy should be read alongside:

- Mobile Phones Policy
-