



Online Safety (E-Safety) and Digital Technology Policy

Policy Owner: Lets Make Change

Version: 1.0

Effective date: 01 June 2026

Review date: June 2027

Approved by: Joseph Fitzpatrick

Version	Date	Author/Reviewed By	Summary of Changes	Approved By	Review Date
1.0	01/06/26	Alex Fitzpatrick	Initial policy created	Joseph Fitzpatrick	June 2027

Let's Make Change (LMC)

Online Safety (E-Safety) and Digital Technology Policy

1. Policy Statement

Let's Make Change (LMC) is committed to ensuring that all learners, staff, volunteers and stakeholders can use digital technologies safely, responsibly and effectively.

Online safety forms an integral part of safeguarding and child protection. LMC recognises that technology provides significant educational benefits but also presents risks including:

- Cyberbullying;
- Online exploitation;
- Inappropriate content;
- Harmful online communication;
- Data breaches;
- Grooming and radicalisation;
- Online fraud and cybercrime.

This policy has been developed in accordance with:

- Keeping Children Safe in Education (KCSIE);
- UK Council for Internet Safety (UKCIS) guidance;
- CEOP recommendations;
- UK GDPR and Data Protection Act 2018;
- Prevent Duty guidance.

2. Scope

This policy applies to:

- All learners attending LMC programmes;
- All staff, tutors, volunteers, and contractors;
- LMC-issued devices;
- Personal devices used for work purposes;
- Online communication platforms;
- Community venues and off-site provision.

3. Vision for Online Safety

LMC's approach is based on two core principles:

Safe to Learn

We want learners to access technology confidently and safely while participating in LMC provision.

Safe for Life

We want learners to develop the skills, awareness, and resilience required to safely navigate digital environments beyond LMC.

4. Educational Benefits of Technology

LMC recognises that technology can:

- Increase learner engagement;
- Support different learning styles;
- Improve accessibility for learners with additional needs;
- Enable collaboration and communication;
- Support personalised learning;
- Provide access to educational resources worldwide;
- Develop digital literacy and employability skills.

5. Roles and Responsibilities

Director

Responsible for:

- Overall oversight of online safety;
- Ensuring appropriate policies and procedures are implemented;
- Responding to significant online safety concerns.

Designated Safeguarding Lead (DSL)

Responsible for:

- Managing online safety concerns;
- Monitoring safeguarding alerts;
- Coordinating referrals where necessary;
- Ensuring online safety forms part of safeguarding procedures.

Staff and Tutors

Responsible for:

- Modelling safe online behaviour;
- Supervising learners appropriately;
- Reporting concerns immediately;
- Following all technology and communication procedures.

Learners

Responsible for:

- Using technology safely and responsibly;
- Following LMC expectations;
- Reporting concerns to trusted adults.

6. Learner Education and Awareness

Learners will receive guidance on:

- Safe internet use;
- Protecting personal information;
- Safe use of social media;
- Cyberbullying;
- Online relationships;
- Privacy settings;
- Online scams and phishing;
- Digital citizenship and responsible behaviour.

7. Managing Information and Data Security

LMC will ensure:

- All staff receive online safety and GDPR training;
- Personal data is handled in accordance with the Data Protection Policy;
- Two-factor authentication is used where available;
- Secure cloud-based storage systems are used;
- Safeguarding information is shared only through approved systems;
- Devices are protected through appropriate security measures.

8. Social Media

Staff Expectations

Staff must:

- Maintain professional boundaries at all times;
- Ensure personal social media use does not compromise their professional role;
- Decline social media contact requests from learners and parents/carers;
- Never discuss learners, families or colleagues online;
- Avoid posting content that may bring themselves or LMC into disrepute.

Learner Expectations

Learners will be supported to:

- Use social media safely;
- Protect their personal information;
- Understand age restrictions and platform requirements;
- Report online concerns promptly.

Parents/carers will be informed where online safety concerns arise.

9. Filtering and Monitoring

LMC uses appropriate filtering and monitoring systems to minimise risk.

Where learners access technology:

- Staff must supervise usage appropriately;
- Learners must not be left unsupervised online;
- Learning activities should be carefully planned;
- Staff devices must remain password-protected and secure.

10. Emerging Technologies

LMC recognises that technology continually evolves.

Before adopting new technologies:

- Educational benefits will be considered;
- Risks will be assessed;
- Appropriate safeguards will be implemented;
- Staff and learners will receive guidance where necessary.

11. Personal Devices

Staff

Staff may use personal devices for work purposes only where authorised and secure.

Staff must:

- Protect devices with passwords or biometric security;
- Ensure devices remain secure at all times;
- Not share devices with learners;
- Report loss, theft or misuse immediately.

Learners

Learners may only use personal devices where authorised by staff.

Where personal device use impacts learning, staff will take appropriate action and provide support to ensure engagement remains positive.

12. Email and Digital Communication

Communication between staff and learners must:

- Use approved LMC communication systems;
- Remain professional at all times;
- Occur during normal working hours wherever possible;
- Be limited to educational purposes.

Staff are encouraged to copy in parents/carers or appropriate colleagues where communication is necessary.

13. Responding to Online Safety Concerns

All online safety concerns must be reported immediately to:

- The DSL;
- Learning Manager;
- Director (where appropriate).

Concerns may include:

- Access to inappropriate content;
- Cyberbullying;
- Online exploitation;

- Grooming concerns;
- Radicalisation;
- Harmful communication;
- Data security concerns.

All incidents must be recorded in accordance with safeguarding procedures.

14. Cyberbullying

LMC maintains a zero-tolerance approach to cyberbullying.

Cyberbullying includes:

- Threatening messages;
- Harassment;
- Online humiliation;
- Sharing harmful content;
- Exclusion through digital platforms.

Where cyberbullying occurs:

- Evidence will be secured;
- Parents/carers will be informed;
- Appropriate sanctions and support will be implemented;
- External agencies, including police may be involved where necessary.

15. Online Exploitation and Grooming

Any concerns regarding:

- Online grooming;
- Sexual exploitation;
- Criminal exploitation;
- Coercion;
- Harmful online relationships;

must be reported immediately to the DSL.

LMC will work with:

- Parents/carers;
- CEOP;
- Police;
- Children's Social Care;
- Other safeguarding agencies.

Where necessary.

16. Incident Response Procedures

Where online safety incidents occur, staff should:

1. Secure and preserve evidence;
2. Ensure learner safety;
3. Inform the DSL immediately;
4. Record concerns using approved systems;
5. Follow safeguarding procedures;
6. Engage external agencies where necessary.

Where there is immediate risk of harm, the DSL must be contacted immediately and safeguarding procedures followed without delay.

17. Staff Training

All staff, tutors, and volunteers will:

- Receive online safety training at induction;
- Complete annual refresher training;
- Receive updates on emerging risks and technologies;
- Understand filtering, monitoring and safeguarding responsibilities.

18. Record Keeping and Confidentiality

Online safety incidents will:

- Be recorded accurately;
- Be stored securely;
- Be reviewed by safeguarding staff;
- Be managed in accordance with GDPR and safeguarding requirements.

19. Monitoring and Review

This policy will be reviewed:

- Annually;
- Following significant incidents;
- Following changes to legislation or statutory guidance;
- Following updates to filtering or monitoring systems.

20. Useful Resources and Guidance

CEOP Safety Centre <https://www.ceop.police.uk>

ThinkUKnow <https://www.thinkuknow.co.uk>

Childnet <https://www.childnet.com>

NSPCC Online Safety <https://learning.nspcc.org.uk>

Parent Zone <https://parentzone.org.uk>

UK Council for Internet Safety <https://www.gov.uk/government/groups/uk-council-for-internet-safety-ukcis>

Keeping Children Safe in Education <https://www.gov.uk/government/publications/keeping-children-safe-in-education>

360 Safe <https://360safe.org.uk>