



ANCHOREACH C.I.C.

Online Safety Policy and Procedures

Policy Owner: Anchoreach C.I.C.

Approved by: Board of Directors

Date Approved: 18/08/2026

Review Date: 18/08/2027

Version: 1.0

1. Policy Statement

Anchoreach C.I.C. recognises that the internet, digital devices, social media and online services are an important part of everyday life, learning, communication and community activity.

Online environments can also expose children, young people, adults at risk, staff and volunteers to risks including inappropriate content, online bullying, grooming, exploitation, scams, fraud, privacy breaches, identity theft and harmful contact.

Anchoreach C.I.C. is committed to promoting safe, responsible and positive use of digital technology while protecting the people who use our services.

Online safety is a shared responsibility. Everyone working with or receiving services from Anchoreach C.I.C. is expected to follow this policy and report concerns promptly.

2. Purpose

This policy and procedure aims to:

- Promote safe and responsible use of the internet and digital technology.
- Protect children, young people and adults who may be at risk from online harm.
- Protect staff, volunteers and directors from inappropriate online activity.
- Reduce the risk of cyberbullying, grooming, exploitation and harmful content.
- Protect personal and confidential information.
- Provide clear procedures for reporting and responding to online safety concerns.
- Support positive digital skills and confidence.
- Ensure online activity is consistent with safeguarding, GDPR and organisational policies.

3. Scope

This policy applies to anyone using digital technology on behalf of or in connection with Anchoreach C.I.C., including:

- Employees.
- Directors.
- Volunteers.
- Tutors and sessional workers.
- Contractors and freelancers.
- Community workers.
- Children and young people participating in activities.
- Adults accessing Anchoreach C.I.C. services.

It applies to online activity undertaken using organisation-owned equipment, personal devices used for organisational purposes, organisational accounts, social media and online communication platforms.

4. Definition of Online Safety

Online safety means taking reasonable steps to protect people from harm when using the internet, computers, tablets, mobile phones, social media, messaging services, online learning platforms and other digital technologies.

Online safety includes protecting people from harmful content, harmful contact, harmful conduct and risks relating to privacy, security and online transactions.

5. Responsibilities

5.1 Board of Directors

The Board is responsible for ensuring appropriate arrangements are in place for online safety.

The Board will:

- Approve and review this policy.
- Ensure significant online safety risks are considered.
- Provide reasonable resources for managing digital risks.
- Review serious incidents and safeguarding concerns.
- Ensure appropriate policies and procedures are maintained.

5.2 Online Safety Lead

The Online Safety Lead will coordinate online safety arrangements and ensure concerns are appropriately managed.

The Online Safety Lead will:

- Monitor online safety concerns.
- Support staff and volunteers.
- Ensure relevant procedures are followed.
- Coordinate training and awareness.
- Review online safety incidents and recommend improvements.

5.3 Staff and Volunteers

Staff and volunteers must:

- Follow this policy and related procedures.
- Use organisational systems responsibly.
- Maintain appropriate professional boundaries.
- Protect personal and confidential information.
- Report online safety concerns immediately.
- Complete relevant training.

5.4 Service Users

Service users will be encouraged and supported to use digital technology safely and responsibly.

6. Acceptable Use of Technology

Digital equipment and internet access provided by Anchoreach C.I.C. should be used responsibly and primarily for legitimate organisational, learning, community or support purposes.

Users must not use organisational equipment or accounts to:

- Access illegal or deliberately harmful material.
- Harass, threaten, bully or intimidate another person.
- Share abusive, discriminatory or offensive material.
- Attempt to access another person's account without permission.
- Download or install unauthorised software.
- Share passwords or authentication information.
- Take, store or distribute inappropriate images or recordings.
- Carry out fraud, scams or other criminal activity.
- Deliberately damage or disrupt digital systems.

7. Passwords and Account Security

Users with organisational accounts must take reasonable steps to keep accounts secure.

- Use strong passwords or passphrases.
- Do not share passwords.
- Do not leave devices unlocked and unattended.
- Use multi-factor authentication where available.
- Report suspected account compromise immediately.
- Do not use another person's account unless specifically authorised.

Passwords should not be written where they can easily be accessed by unauthorised people.

8. Personal Information and Privacy

Personal information must be handled in accordance with Anchoreach C.I.C.'s GDPR and Data Protection Policy.

- Only collect information that is necessary.
- Keep personal information secure.
- Do not share personal information without a lawful and appropriate reason.
- Avoid sending sensitive information through insecure channels.
- Check recipients carefully before sending emails or messages.
- Report suspected data breaches immediately.

Particular care must be taken when handling information about children, young people and adults at risk.

9. Social Media

Staff, volunteers and directors should maintain professional boundaries when using social media in connection with their work.

They must not:

- Use personal social media to form inappropriate relationships with service users.
- Post confidential information about service users, staff, volunteers or the organisation.
- Share photographs or videos of service users without appropriate consent and authorisation.
- Post content that could place a service user at risk.
- Represent personal views as official organisational statements unless authorised.

Official Anchoreach C.I.C. social media accounts must only be managed by authorised individuals.

10. Photographs, Videos and Recording

Photographs, videos or recordings involving service users must only be made and used where appropriate consent, safeguarding arrangements and organisational requirements have been met.

Staff and volunteers must not use personal devices to record children, young people or adults at risk unless this has been specifically authorised.

Images must be stored and shared securely and only for agreed purposes.

11. Online Communication with Service Users

Communication with service users should take place through approved organisational channels wherever possible.

- Professional boundaries must be maintained.
- Communication should be appropriate, respectful and relevant.
- Private or secret communication with children or adults at risk is not appropriate.
- Staff and volunteers should not delete relevant communications where they may be needed for safeguarding or organisational records.

Where communication with a child or young person is required, safeguarding procedures and appropriate professional boundaries must be followed.

12. Children and Young People

Children and young people may face additional online risks including grooming, exploitation, cyberbullying, harmful content, inappropriate contact and pressure to share images.

Anchoreach C.I.C. will promote age-appropriate online safety awareness and will respond to concerns in accordance with safeguarding procedures.

Where online activity is part of a session, staff should consider appropriate supervision, privacy settings, content filtering and the age and needs of participants.

13. Adults Requiring Additional Support

Some adults may require additional support to use digital technology safely.

Staff and volunteers should consider communication needs, digital confidence, vulnerability to scams, exploitation, financial abuse, privacy and the individual's ability to recognise online risks.

Support should be proportionate and should promote independence wherever possible.

14. Cyberbullying and Online Harassment

Cyberbullying, harassment, threats and discriminatory behaviour are not acceptable.

Concerns should be reported to a member of staff or manager.

Where appropriate, evidence such as screenshots, messages or links should be retained without forwarding harmful material unnecessarily.

Serious threats, abuse or safeguarding concerns must be escalated in accordance with relevant procedures.

15. Grooming, Exploitation and Inappropriate Contact

Online grooming or exploitation may involve someone building trust or a relationship in order to manipulate, control or exploit another person.

Warning signs may include secretive online relationships, requests for personal information or images, pressure to move conversations to private platforms, threats, blackmail or unexplained changes in behaviour.

Any concern that a child, young person or adult at risk may be experiencing online grooming or exploitation must be reported immediately under the Safeguarding Policy and Procedures.

16. Online Content

Users should take care when accessing online content.

Staff and volunteers should not deliberately expose service users to content that is inappropriate for their age, needs or circumstances.

If inappropriate, illegal or harmful content is encountered accidentally, the user should stop accessing it and report the concern where appropriate.

Staff should not investigate potentially illegal material themselves.

17. Email and Messaging

Email and messaging systems must be used responsibly.

- Check addresses and recipients before sending.
- Be cautious with links and attachments.
- Do not open suspicious attachments.
- Do not respond to suspected phishing messages.
- Report suspicious messages to the appropriate person.
- Use appropriate professional language.

- Avoid sending unnecessary personal or sensitive information.

Where a message may contain safeguarding or legal information, staff should follow organisational procedures for secure communication and record keeping.

18. Phishing, Scams and Fraud

Users should remain alert to phishing emails, fake websites, impersonation, online scams and requests for money or personal information.

Warning signs may include unexpected requests, urgent demands, unusual payment instructions, suspicious links, spelling or formatting errors, and requests to bypass normal procedures.

If a user believes they have responded to a scam or disclosed information, they must report it immediately so that appropriate action can be taken.

19. Mobile Devices and Personal Devices

Where personal devices are used for organisational purposes, users must take reasonable steps to protect information and maintain professional boundaries.

- Use device security such as a PIN, password or biometric protection.
- Keep operating systems and applications updated.
- Do not allow unauthorised people to access organisational information.
- Do not store unnecessary personal information on personal devices.
- Report loss or theft of a device containing organisational information immediately.

20. Remote and Online Sessions

Where Anchoreach C.I.C. delivers online sessions, the session leader should consider:

- Who is attending.
- Whether participants are known to the organisation.
- Appropriate privacy and security settings.
- Whether the session should be recorded.
- How participants can report concerns.
- How personal information will be protected.
- Whether additional safeguarding controls are required.

Online sessions should be conducted using approved platforms where possible.

21. Online Meetings and Professional Boundaries

Staff and volunteers should conduct online meetings in an appropriate environment and maintain professional standards.

- Use an appropriate display name and profile.
- Avoid sharing unnecessary personal information.
- Use appropriate backgrounds and surroundings.
- Maintain professional language and behaviour.
- Do not record meetings unless authorised and participants have been informed where required.

22. Incident Reporting Procedure

Any online safety concern should be reported as soon as possible.

Examples include:

- Cyberbullying.
- Threats or harassment.
- Grooming or exploitation.
- Inappropriate contact.
- Inappropriate images or content.
- Loss or theft of a device.
- Suspected phishing or fraud.
- Account compromise.
- Unauthorised access.
- Data breaches.
- Safeguarding concerns.

Procedure

1. Take reasonable steps to protect immediate safety.
2. Do not confront or investigate the person responsible.
3. Preserve relevant evidence where safe and appropriate.
4. Report the concern to the manager, Online Safety Lead or Safeguarding Lead.
5. Record the concern accurately.
6. Escalate to emergency services or other appropriate authorities where required.
7. Review the incident and identify any further action or learning.

23. Safeguarding and Online Safety

Online safety concerns involving children, young people or adults at risk must be managed in accordance with Anchoreach C.I.C.'s Safeguarding Policy and Procedures.

Staff and volunteers must not promise confidentiality where a safeguarding concern is disclosed.

If there is an immediate risk of serious harm, emergency services should be contacted as appropriate.

24. Data Breach Procedure

A suspected data breach must be reported immediately to the appropriate manager or responsible person.

Examples include lost devices, emails sent to the wrong recipient, stolen passwords, unauthorised access or accidental disclosure of personal information.

The organisation will assess the incident and take appropriate steps in accordance with its GDPR and Data Protection Policy.

25. Training

Staff and volunteers who use digital technology as part of their role will receive appropriate online safety information or training.

Training may include:

- Online safeguarding.
- Cyberbullying and harassment.
- Grooming and exploitation.
- Phishing and scams.
- Password and account security.
- Data protection.
- Social media and professional boundaries.
- Incident reporting.
- Safe use of digital devices.

26. Monitoring and Review

Anchoreach C.I.C. will monitor online safety through reported incidents, safeguarding concerns, feedback, training records, data breaches and reviews of digital practices.

Serious incidents will be reviewed to identify whether additional controls, training or changes to procedures are required.

27. Online Safety Quick Checklist

Before using digital systems

- ☐ Use an appropriate account and device.
- ☐ Ensure passwords and security measures are in place.
- ☐ Check privacy and security settings.
- ☐ Consider whether personal information is being shared.

During online activity

- ☐ Maintain professional boundaries.

- ☐ Do not share confidential information unnecessarily.
- ☐ Be alert to scams, inappropriate contact and harmful content.
- ☐ Report concerns promptly.

If something goes wrong

- ☐ Protect immediate safety.
- ☐ Do not investigate serious concerns yourself.
- ☐ Preserve relevant evidence where appropriate.
- ☐ Report the incident.
- ☐ Record what happened.
- ☐ Follow safeguarding and data protection procedures.

28. Online Safety Incident Flowchart

Online safety concern identified

↓

Is anyone at immediate risk of harm?

→ **Yes:** Take immediate safety action and contact emergency services where necessary.

→ **No:** Continue with the reporting procedure.

↓

Report to manager / Online Safety Lead / Safeguarding Lead

↓

Record the concern and preserve relevant evidence

↓

Assess safeguarding, data protection and other risks

↓

Take appropriate action and make any required external referral

↓

Review incident and update controls or training where necessary

29. Records

Anchoreach C.I.C. may maintain:

- Online safety incident records.
- Safeguarding records.

- Data breach records.
- Training records.
- Risk assessments.
- Relevant consent records.

Personal information will be stored securely and managed in accordance with the organisation's GDPR and Data Protection Policy.

30. Non-Compliance

Failure to follow online safety procedures may place individuals or the organisation at risk.

Where a person repeatedly fails to follow agreed procedures, Anchoreach C.I.C. may provide additional training, supervision or take other appropriate action.

Serious breaches may result in removal of access to systems, ending of a volunteer placement, disciplinary action where applicable, or referral to appropriate authorities.

31. Policy Review

This policy and procedure will be reviewed at least annually or sooner where:

- A serious online safety incident occurs.
- A safeguarding concern identifies a new online risk.
- Digital systems or platforms change.
- New activities are introduced.
- There are significant changes to legislation or guidance.
- Staff, volunteer or service-user feedback identifies a need for change.

32. Approval

Approved by: Board of Directors

Signature: P Marriner

Name: Paul Marriner

Position: Managing Director

Date: 18/08/2026

Review Date: 18/08/2027