

Online Safety Policy

Cirk Hes Ltd.

www.cirkhes.co.uk

Cirk Hes, F8 Helston Business Park, Clodgey Lane, Helston, TR13 8FZ

Email: info.cirkhes@gmail.com - Charity No. 01106043 - Company No. 0484997

Website <https://www.cirkhes.co.uk>

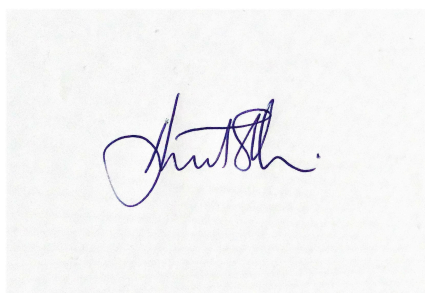
Policy Owner: Ross Wheeler (SEND Lead)

Approved By: Naomi Lewis (Charity Manager) on behalf of the Cirk Hes Ltd Board of Trustees

Date Approved: 15-07-26

Reviewed and approved by the Board 18/09/2026 authorised by Mr David Ellis

Version: 1.0



1. Purpose

Cirk Hes recognises that digital technology and online communication play an important role in delivering our services, engaging with communities, supporting volunteers, and communicating with children, young people, families, and vulnerable adults.

While technology provides many benefits, it also presents safeguarding, privacy, security, and wellbeing risks.

This policy sets out how we will promote safe, responsible, and appropriate use of digital technology and online platforms to protect everyone involved with our organisation.

2. Scope

This policy applies to:

- Trustees
- Employees
- Volunteers
- Freelance and sessional workers
- Students and work placements
- Anyone acting on behalf of the organisation

It applies whenever individuals use:

- Organisation-owned equipment
 - Personal devices for organisation business
 - Email
 - Websites
 - Social media
 - Video conferencing
 - Messaging applications
 - Online learning platforms
 - Cloud storage
 - Digital records
-

3. Policy Statement

Cirk Hes is committed to:

- Protecting children, young people and vulnerable adults online.
 - Promoting positive, safe and respectful online behaviour.
 - Preventing abuse, exploitation, bullying and harassment online.
 - Protecting personal information.
 - Ensuring safe use of digital communication.
 - Responding promptly to online safeguarding concerns.
 - Complying with UK data protection legislation.
-

4. Legal Framework

This policy supports compliance with:

- UK GDPR
 - Data Protection Act 2018
 - Children Act 1989 and 2004
 - Care Act 2014
 - Counter-Terrorism and Security Act 2015 (PREVENT)
 - Safeguarding Vulnerable Groups Act 2006
 - Online Safety Act 2023 (where applicable)
-

5. Principles

Everyone using technology on behalf of the organisation should:

- Treat others with respect.

- Protect confidential information.
 - Use digital communication professionally.
 - Report concerns promptly.
 - Respect privacy.
 - Follow safeguarding procedures.
 - Use organisation systems responsibly.
-

6. Responsibilities

Managing Staff and the Board of Trustees

Trustees will:

- Approve this policy.
 - Ensure suitable safeguarding arrangements are in place.
 - Support safe digital working.
 - Review the policy annually.
-

Designated Safeguarding Lead (DSL)

The DSL will:

- Respond to online safeguarding concerns.
 - Record incidents.
 - Make referrals where necessary.
 - Support staff and volunteers.
 - Review online safety practices.
-

Staff and Volunteers

All staff and volunteers must:

- Follow this policy.
 - Complete safeguarding and online safety training.
 - Protect passwords.
 - Report online concerns.
 - Use professional communication methods.
 - Respect confidentiality.
-

7. Safe Online Communication

Staff and volunteers should:

- Use organisation email addresses wherever possible.

- Use organisation-approved messaging systems.
- Keep communication professional.
- Maintain appropriate boundaries.
- Avoid private or secret communication with children or vulnerable adults.
- Copy another authorised adult into messages where appropriate.
- Keep communication relevant to organisational activities.

Where communication with young people is necessary, parents or carers should be informed where appropriate and communication should follow organisational procedures.

8. Social Media

The organisation encourages responsible use of social media.

Staff and volunteers must not:

- Share confidential information.
- Post images without permission.
- Discuss safeguarding concerns online.
- Engage in online arguments with service users.
- Contact children or vulnerable adults using personal social media accounts.
- Represent personal opinions as those of the organisation.

Organisation social media accounts should only be managed by authorised individuals.

9. Photography, Video and Live Streaming

Photographs or videos should only be taken:

- With appropriate consent.
- For legitimate organisational purposes.
- Using organisation-approved devices wherever possible.
- In line with safeguarding guidance.

Images should never:

- Identify children by full name alongside their image unless explicit consent has been obtained.
- Be stored on personal devices unless authorised.
- Be shared via personal messaging services.

Live streaming activities require prior risk assessment and appropriate supervision.

10. Video Meetings

When using online meeting platforms:

- Meetings should be scheduled through official accounts where possible.

- Participants should know who is attending.
 - Meetings involving children or vulnerable adults should, wherever possible, involve at least two responsible adults or be conducted in an open and transparent way.
 - Recording should only occur where necessary and with consent.
 - Appropriate privacy settings should be used.
-

11. Personal Devices (Bring Your Own Device)

Where personal devices are used for organisational work:

Users should:

- Protect devices with passwords or biometric security.
- Keep software updated.
- Use secure internet connections.
- Report lost or stolen devices used for organisational work.
- Delete organisational information when no longer required.

Sensitive information should not be permanently stored on personal devices.

12. Cyber Security

Everyone should:

- Use strong passwords.
 - Enable multi-factor authentication where available.
 - Keep software updated.
 - Lock devices when unattended.
 - Report phishing emails.
 - Never share passwords.
 - Store documents securely.
 - Back up important information where appropriate.
-

13. Online Safeguarding Risks

Online risks may include:

- Cyberbullying
- Grooming
- Sexual exploitation
- Financial exploitation
- Radicalisation
- Identity theft

- Fraud and scams
- Online harassment
- Sharing harmful or illegal content
- Exposure to inappropriate material

Staff should remain alert to these risks when supporting service users.

14. Artificial Intelligence (AI)

Where AI tools are used:

- Confidential or personal information must not be entered into public AI systems unless authorised and lawful.
 - AI-generated content should always be checked by a member of staff before use.
 - AI should support, not replace, professional judgement.
 - Safeguarding decisions must never be made solely by AI.
-

15. Reporting Online Safety Concerns

Anyone who becomes aware of an online safety concern should:

1. Preserve evidence where appropriate.
2. Avoid deleting messages or images unless advised.
3. Report concerns immediately to the Designated Safeguarding Lead.
4. Record factual information.
5. Follow the organisation's safeguarding procedures.

If a child or adult is believed to be at immediate risk of harm, emergency services should be contacted on 999.

16. Confidentiality and Data Protection

Personal information must be:

- Collected lawfully.
- Stored securely.
- Shared only where appropriate.
- Accessed only by authorised individuals.
- Deleted in accordance with organisational retention policies.

Everyone must comply with the organisation's Data Protection Policy.

17. Training

All staff and volunteers will receive appropriate training covering:

- Online safeguarding.

- Safe digital communication.
- Cyber security awareness.
- Social media use.
- Data protection.
- Recognising online abuse.
- Reporting concerns.

Refresher training should be completed regularly.

18. Breaches of this Policy

Failure to follow this policy may result in:

- Additional training.
- Supervision or management action.
- Disciplinary procedures where appropriate.
- Referral to statutory agencies if safeguarding concerns arise.

Serious breaches may be reported to relevant authorities.

19. Related Policies

This policy should be read alongside:

- Safeguarding Children Policy
 - Safeguarding Adults Policy
 - Code of Conduct
 - Data Protection Policy
 - Equality, Diversity and Inclusion Policy
 - Whistleblowing Policy
 - PREVENT Policy
 - Complaints Policy
-

20. Monitoring and Review

The Board of Trustees and Designated Safeguarding Lead will review this policy annually or sooner if:

- Legislation changes.
- Guidance is updated.
- An online safeguarding incident occurs.
- New technology or working practices are introduced.