Horserenity CIC

E-Safety, Online Safety, Acceptable Usage, and Mobile/Smart Technology Policy

Date of Issue: 02.12.2025
Review Date: 01.12.2026

Created by: Dan Vivian

Reviewed by: Sarah Vivian

1. Introduction

Horserenity CIC is committed to ensuring that all children, young people, vulnerable adults, staff, and volunteers are kept safe from online risks. Although activities primarily take place onsite and in person, digital tools—including mobile phones, smart devices, online communication, social media, and digital record-keeping—play an increasing role in our operations.

This policy sets out clear expectations for safe, responsible, and lawful use of technology by all individuals connected with the centre. It supports compliance with UK legislation and best-practice safeguarding standards.

2. Purpose of the Policy

This policy aims to:

- Promote safe and responsible use of digital technology.
- Protect children and young people from online risks, exploitation, and inappropriate content.
- Provide clear guidance on the use of mobile phones, smart devices, photography, and digital communication at Horserenity CIC.
- Ensure compliance with GDPR, the Data Protection Act 2018, the Online Safety Act 2023, and general safeguarding requirements.
- Protect staff and volunteers by establishing clear professional boundaries.
- Prevent misuse of digital media, images, and personal information.

3. Scope

This policy applies to:

- All staff (paid or unpaid)
- Volunteers and apprentices
- Directors
- Contractors and visiting professionals
- Children, young people, and adult participants
- Parents, carers, and visitors where relevant

This policy covers the use of:

- Mobile phones and smart watches
- Cameras and audio-visual recording devices
- Social media and messaging platforms
- Email and digital communication
- Online platforms used for administration or learning
- Website content, marketing, and digital storage of information

4. Principles of E-Safety and Online Safety

Horserenity CIC is committed to:

- Creating a safe digital environment for children and young people.
- Ensuring that online behaviour reflects our values of respect, responsibility, and safeguarding.
- Keeping personal data secure and confidential.
- Ensuring that digital communication with children is transparent, appropriate, and always via approved channels.
- Ensuring parents and carers are informed of how their children's data and images may be used.

5. Acceptable Use Requirements

5.1 Staff and Volunteers

Staff and volunteers must:

- Use digital devices and communication tools **only for professional purposes**.
- Keep work-related digital information secure and password-protected.
- Use only Horserenity CIC-approved platforms for communication.

- Never share personal phone numbers, personal social media profiles, or private messaging channels with under-18s or vulnerable adults.
- Report any e-safety or online safety concern promptly to the Designated Safeguarding Lead.
- Not access inappropriate, illegal, discriminatory, or harmful content using any device on site.

Professional Boundaries

Staff and volunteers must not:

- Engage with current or recent participants under 18 via personal social media.
- Post images or information about participants on personal accounts.
- Use personal devices to store participant data or images.
- Allow participants access to their personal phones or smart devices.

5.2 Children and Young People

Participants may only use mobile phones or smart devices on site with staff permission.

They must not:

- Access inappropriate content.
- Use devices around horses unless supervised and safe.
- Use personal devices to contact staff or volunteers.

5.3 Parents and Carers

Parents/carers must not:

- Take photos or videos of other children or staff without consent.
- Share images from sessions on social media that include other participants.
- Use mobile phones during sessions unless authorised for safety reasons.

6. Use of Mobile Phones, Smart Watches, Cameras, and Recording Devices

6.1 Staff Device Use

- Personal phones must be kept on silent during sessions and used only when necessary.
- Work-related calls should be made using approved contact numbers where possible.

- Staff may only use centre-approved devices to capture photos or footage for official purposes. These can be personal devices.
- At the end of sessions content is uploaded to a secure site and permanently deleted from the personal device.

6.2 Photography and Video of Participants

Photography or filming may only occur when:

- It is necessary for educational, safety, monitoring, or promotional purposes.
- Consent has been fully and clearly obtained from parents/carers and participants (where appropriate).
- Images are stored securely and used solely for the purpose consented to.
- Faces of children are not posted on public digital platforms without explicit written consent.

6.3 Smart Watches and Wearable Tech

Smart watches must not be used to:

- Take photos or videos
- Record audio
- Access the internet unsupervised

Children may wear smart watches for health or medical monitoring only with parental agreement.

7. Digital Communication

7.1 Communication with Children and Young People

Communication must always be:

- Professional
- Transparent
- Through approved platforms (e.g., official email, centre communication system)
- Logged where appropriate

Staff must **never** send or respond to:

- Personal messages
- Private chats
- Social media friend requests

7.2 Communication with Parents/Carers

Digital communication may include:

- Email
- Text or messaging for scheduling and logistics
- Updates via official social media pages

Messages must be factual, not emotional in tone, and always professional.

8. Social Media Use

8.1 Official Channels

Only authorised staff may post to:

- Horserenity CIC’s official website
- Official Facebook, Instagram, or other pages

Content must:

- Follow safeguarding and consent rules
- Reflect organisational values
- Never identify vulnerable individuals without consent
- Avoid sharing location in real time when children are present

8.2 Personal Social Media

Staff, volunteers, and participants may not:

- Post images of sessions that include children or young people without consent
- Tag or identify participants without permission
- Discuss incidents, behaviour, or internal matters
- Share confidential or sensitive information

9. Online Safety Risks

Risks include:

- Exposure to inappropriate content
- Grooming or exploitation
- Cyberbullying
- Sharing personal information
- Misuse of images
- Identity theft or data breaches

Staff must remain vigilant and report concerns immediately.

10. Data Protection and Security

Horserenity CIC complies with:

- GDPR (UK GDPR)
- Data Protection Act 2018

This includes:

- Secure handling of digital records
- Restricted access to personal data
- Regular review of data security
- Secure deletion of digital files no longer required

11. Responding to E-Safety Concerns

Any concerns or incidents—such as misuse of devices, inappropriate content, or disclosure of online harm—must be reported to the:

Designated Safeguarding Lead (DSL):
Sarah Vivian
Email: sarah@horserenity.co.uk

Phone: 07734 058783

Serious concerns may be referred to:

- Local Authority Safeguarding Teams
- Police
- The Internet Watch Foundation
- NSPCC helplines

A record of the incident must be made in accordance with safeguarding procedures.

12. Training and Awareness

Horserenity CIC will ensure that:

- All staff and volunteers receive e-safety and digital safeguarding training.
- Children and young people are encouraged to learn safe online behaviour.
- Parents/carers are informed of digital safety expectations.

13. Policy Breaches

Breaches of this policy may lead to:

- Restriction of device use
- Parental involvement (regarding children/young people)
- Disciplinary action for staff or volunteers
- Referral to external authorities where necessary

14. Review of Policy

This policy will be reviewed annually by the Board of Directors or earlier if required due to:

- Legislative changes
- Digital practice updates
- Safeguarding developments