Genuine Futures CIC – Online Safety Policy

PREVENTION OVER PUNISHMENT: BUILDING SAFER FUTURES TOGETHER

Version: 1.0 Approved by Board: 01 Nov 2025 Next Review: 01 Nov 2026

1. Policy Statement

Genuine Futures CIC recognises that digital communication and online technology are central to modern education, social engagement, and organisational operations. We are committed to ensuring that all online activity involving staff, volunteers, participants, and partners is conducted safely, ethically, and in accordance with UK law. This policy sets out the standards and expectations for online safety, digital safeguarding, and responsible technology use.

2. Legislative Framework

This policy aligns with the following UK legislation and statutory guidance:• Data Protection Act 2018 and UK GDPR• Keeping Children Safe in Education (KCSIE) 2025• Working Together to Safeguard Children (2023)• Computer Misuse Act 1990• Malicious Communications Act 1988• Communications Act 2003• Equality Act 2010• ICO Guidance on AI and Data Protection (2023)• DfE Standards for Digital and Technology in Schools (2024)

3. Scope and Purpose

This policy applies to all staff, trustees, volunteers, contractors, and participants using Genuine Futures CIC digital systems or online communication tools. It covers organisational websites, social media, virtual learning environments, AI tools, video conferencing, and online collaboration platforms. The purpose is to ensure responsible, lawful, and secure digital practice across all Genuine Futures CIC activities.

4. Roles and Responsibilities

• Board of Directors: Holds overall accountability for ensuring compliance with online safety and data protection legislation.• Designated Safeguarding Lead (DSL): Oversees online safety incidents and ensures prompt action in line with safeguarding procedures.• Staff and Volunteers: Must follow all online safety procedures, report incidents promptly, and complete regular training.• Participants and Service Users: Expected to use digital platforms responsibly, following guidance provided by staff or volunteers.

5. Acceptable Use of Technology

All users must adhere to the following principles:• Use Genuine Futures CIC technology and accounts only for authorised purposes.• Do not share personal, confidential, or sensitive information online without consent.• Do not download or share inappropriate, illegal, or offensive material.• Protect passwords and do not allow unauthorised access to accounts.• Ensure communication remains professional, appropriate, and transparent.

6. Online Communication and Social Media

Online communication should uphold the same professional standards as face-to-face interactions. • Official accounts must only be used for organisational purposes. • Staff and volunteers must not 'friend' or privately message children, young people, or service users through personal social media accounts.• All public

communications should reflect **Genuine Futures CIC's** values and avoid political, discriminatory, or offensive content.• Consent must be obtained before publishing any identifiable images or personal information online.

7. Digital Safeguarding for Children and Adults at Risk

Genuine Futures CIC is committed to protecting children, young people, and adults at risk in all online environments. This includes:• Educating participants about online risks and digital resilience.• Using secure, moderated platforms for communication and collaboration.• Ensuring that all online sessions involving children are supervised by trained staff or volunteers.• Reporting online abuse, exploitation, or cyberbullying in line with the Safeguarding and Child Protection Policy.

8. Cybersecurity and Data Protection

To protect organisational and personal data:• Devices must be password-protected and encrypted where possible.• Sensitive data must not be shared over unsecured channels.• Users must not install unauthorised software or connect to unsecured Wi-Fi networks for work activities.• Any suspected cyberattack or data breach must be reported immediately to the Data Protection Lead and DSL.• Regular audits and updates will be conducted to ensure compliance with UK GDPR and ICO standards.

9. Responsible Use of AI and Emerging Technologies

Genuine Futures CIC supports the ethical and innovative use of artificial intelligence (AI) and digital technologies to enhance learning and community engagement. All use of AI tools must comply with UK GDPR and safeguarding principles. The following standards apply:• AI tools must not process or store sensitive, identifiable, or confidential information about staff, volunteers, or participants.• All outputs generated by AI systems should be reviewed by a responsible staff member before being shared publicly.• Transparency must be maintained—individuals must be informed when AI systems are used in learning or communication contexts.• Staff and volunteers must receive periodic training on emerging technology use and associated risks.

10. Reporting Online Concerns

All online safety incidents must be reported immediately to the Designated Safeguarding Lead (DSL). This includes concerns such as cyberbullying, online abuse, data breaches, or inappropriate content. If a person is at immediate risk of harm, contact emergency services (999) and notify the DSL as soon as possible. All incidents will be recorded securely and handled in accordance with the Safeguarding and Data Protection Policies.

11. Monitoring and Review

This policy will be reviewed annually or sooner if required by legislative updates or new digital risks. The review will include consultation with safeguarding leads, IT advisors, and the Board to ensure that procedures remain effective and compliant.Last reviewed: [Insert Date]Next review due: [Insert Date + 12 months]

12. Linked Policies

• Safeguarding & Child Protection Policy• Data Protection & Privacy Policy• Volunteer Policy• Equality, Diversity & Inclusion Policy• Health & Safety Policy

Appendix: Online Safety Reporting Contacts

• Designated Safeguarding Lead (DSL): Mike Alleyne Contact mike@genuinefutures.co.uk• Deputy DSL: Charlotte Hamblet Contact charlotte@genuinefutures.co.uk • Data Protection Lead: [Insert Name / Contact Details]• Local Authority Designated Officer (LADO): [Insert Contact Information]• Adult Safeguarding Board Contact: [Insert Contact Information]• Emergency Services: 999• Non-Emergency Police Contact: 101• Internet Watch Foundation (IWF): https://www.iwf.org.uk• UK Safer Internet Centre: https://www.saferinternet.org.uk