



Digital Safety Policy

Purpose and Scope

Growing Resilience in Teens (GRIT), a Charitable Incorporated Organisation (CIO), registered charity number 1176272, recognises the importance of raising awareness of child protection and safeguarding issues associated with online platforms.

This policy should be read in conjunction with our policy on photography and images, and our safeguarding policy. All volunteers and staff are trained annually in child safeguarding, and this includes training in online grooming. We acknowledge the use of some relevant material from The National Online Safety Guides and the NSPCC guidance.

Much has been written about online safety but it is beyond the scope of this policy to provide comprehensive guidance on all the many aspects of the online world. We advise all employees and mentors to use the appended online national guidelines, in addition to this policy and our in-house training programmes.

1. Aims

The aims of this policy are to:

- Enable and encourage employees, volunteers and young people involved in GRIT activities to use agreed social media and online meeting spaces to facilitate both training, mentoring and running the GRIT programme.
- Help children, staff and volunteers understand how to use the internet and social media platforms safely, as they apply to GRIT;

2. Application

This policy applies to everyone associated with GRIT who may use online platforms in connection with the charity's work. This includes:

- Trustees
- Self-employed staff and contractors
- Volunteers
- Young people participating in GRIT programmes
- Parents and guardians where their contact details are used for programme communication

It covers the use of GRIT-approved platforms, including:

- **MS Teams** – for online meetings and management discussions
- **Zoom** – for programme delivery where required
- **WhatsApp** – for programme-related communication with young people and families

3. Training and Awareness

- All volunteers and self-employed staff complete annual Child Safeguarding training, which includes online safety and online grooming awareness.
- Trustees complete basic training in data protection and online safety to ensure appropriate governance oversight.
- Updates on new risks, platforms, or online behaviours will be included in refresher training or team briefings as required.

4. General Guidelines for online safety

- Keep Personal Information to a minimum
- Keep Your Privacy Settings On
- Practice Safe Browsing
- Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection where possible
- Be Careful What You Download
- Choose Strong Passwords
- Make Online Purchases From Secure Sites
- Be Careful What You Post
- Be Careful Who You Meet Online
- Keep Your Antivirus Program Up To Date.

5. Considerations for GRIT teenagers

All GRIT teenagers have access to a mobile phone on entry to the programme. All take part in several GRIT WhatsApp groups when the service is delivered face-to-face through weekly boxing/coaching sessions. Where a teenager doesn't have access to a mobile phone, we discuss this with the parent or guardian and may need to use the parent's contact details to relay messages. Using WhatsApp is therefore an inclusive activity for GRIT teens.

Parents are fully briefed about the programme. Where a participant is under 16, **explicit written consent from the parent or guardian is required** for the use of WhatsApp and all other online elements of the programme. This consent is recorded and stored securely in line with GRIT's Data Protection Policy.

With the move to a virtual programme at the outset of the Coronavirus pandemic in March 2020, all teens on the programme were contacted about their engagement with online delivery. All of them had access to either a computer or a smartphone to join Zoom meetings, and the majority chose to participate from their own bedrooms. On occasions where a participant lost connectivity on Zoom, they were advised to message the group leader on WhatsApp to resolve the issue. Group meetings were re-established in September 2020.

In line with GRIT's commitment to creating a respectful, safe, and inclusive environment, young people may be removed from WhatsApp groups if their behaviour is not in line with GRIT's values, Code of Conduct, or safeguarding expectations.

6. Risk Management

- **Regular Reviews**

Risk assessment meetings take place at least monthly and involve senior management.

- **Concerns During the Virtual Programme**

At the start of the Coronavirus pandemic, concerns were raised about our ability to follow up with teenagers who might be adversely affected. To address this, we developed a multi-stranded approach to support:

- **One-to-one support** for the most vulnerable, available during weekly boxing/coaching sessions and continued via WhatsApp or occasional phone calls during lockdown.
- **Small group approach** – the programme runs with a maximum of 12 participants, allowing flexible, targeted support.

- **Initial Assessments**

All new participants completed online assessments, which were reviewed by GRIT's founder (a qualified GP) before entry to the programme. This process continued during lockdown.

- **NHS Partnership**

Since 2021/2022, health and well-being coaches from our NHS partnership check all new referrals. Any concerns are raised in weekly Multi-Disciplinary Team (MDT) meetings.

7. Technological Aspects of Digital Security

Organisation

All GRIT staff are self-employed on renewable contracts. GRIT provides laptops to all contractors; however, personal laptops may also be used for GRIT work provided they meet the same security standards.

- **GRIT laptops** are password-protected, set to auto-lock, and configured so that no personal or identifiable data is stored locally. All files must be saved in GRIT's secure shared drive, which is protected by security software and managed by our IT partner, IdeasAnvil. Each contractor is issued with a Microsoft 365 licence via IdeasAnvil. GRIT laptops remain the property of GRIT at all times.
- **Personal laptops used for GRIT work** must be password-protected, set to auto-lock, and run up-to-date operating system and security patches. Approved antivirus/anti-malware software must be installed, encrypted storage used where available, and the device used only by the contractor. No GRIT personal or identifiable data may be stored locally; all files must be saved in the secure shared drive.

8. Privacy Settings and Regulations

GRIT uses Facebook, Instagram, and YouTube for general posts only. Content uses library photos or images that meet our Photography and Use of Images Policy. All posts are created and shared only by the GRIT admin team.

9. Approved Platforms

- **MS Teams** – used for management meetings and discussions with external agencies.
- **Zoom** – used for programme delivery when required; all meetings are password-protected.
- **WhatsApp** – used for programme communication with young people. For anyone under 16, explicit written consent from a parent or guardian is required.

10. Moderation

GRIT does not use open social media platforms or chat room services for group conversations. WhatsApp groups are monitored and moderated by staff in line with our Code of Conduct and Safeguarding Policy. Young people may be removed from a group if their behaviour does not meet GRIT's expectations.

11. Safeguarding

Our safeguarding policy was reviewed in 2025 to cover online delivery of the GRIT programme. As the sessions were delivered by Zoom in a live setting with the boxing coach and the programme director, nobody had access to the teenagers online. Our safeguarding policy is currently reviewed annually.

12. National Guidelines

We recommend referring to trusted UK e-safety resources, which provide up-to-date guides, toolkits, and training materials for children, parents, and professionals:

- Internet Matters — practical advice and downloadable resources:
<https://www.internetmatters.org/resources/esafety-leaflets-resources/>
- Childnet — resources and toolkits for children, parents, and schools:
<https://www.childnet.com/>
- UK Safer Internet Centre — guidance and advice for safe and responsible internet use:
<https://saferinternet.org.uk/>
- NSPCC Online Safety — training and guidance for parents and professionals:
<https://learning.nspcc.org.uk/research-resources/online-safety-resources>

13. Related Policies

This policy should be read in conjunction with the following GRIT Policies, which provide additional guidance and context.

- GRIT Photography policy
- GRIT Safeguarding Policy
- GRIT Data Security & Cyber Safety Policy – covers system access, secure handling of data, and cyber risks.
- GRIT Confidentiality Policy – outlines responsibilities for handling sensitive information.
- GRIT Code of Conduct – sets expected behaviours for staff, volunteers, and young people online and offline.
- GRIT IT Acceptable Use Guidelines – details safe use of devices, emails, and online platforms.
- GRIT Social Media Policy – guidance on appropriate use of organisational and personal accounts when representing GRIT.

-
- Updated by James O'Mara (Finance and Operations Manager 9/4/25)
 - Approved by Dr Louise Randall, Chairman

Signature:

Date:

Dr Louise Randall

26/09/2025

- Next review date: 1/4/26