Data Security & Cyber Security Training Needs Analysis Policy

Purpose and Scope

This policy sets out Growing Resilience in Teens' (GRIT, CIO registered number 1176272) commitment to maintaining robust data security and cyber safety. It establishes role-specific responsibilities and mandatory training to protect sensitive personal data and uphold safeguarding obligations. It applies to all individuals associated with GRIT, including part-time self-employed staff, trustees, and third-party representatives who have access to GRIT systems, data, or digital infrastructure. This includes contractors, volunteers, and any partner organisations who may be given access to GRIT's systems or data.

Given the nature of GRIT's work with young people, including safeguarding responsibilities and handling of sensitive personal data, this policy aims to mitigate the risks associated with unauthorised access, data loss, or cyber threats. This is achieved through targeted training and ongoing monitoring of security awareness.

1. **Staff Structure and Access Summary**

GRIT currently consists of the following roles:

- **CEO** (part-time, self-employed)
- **Chairman** (Trustee)
- **Trustees**
- **Operations & Finance Manager** (part-time, self-employed)
- **Meetings Coordinator/Administrator** (part-time, self-employed)
- **10 Part-Time Coaches** (self-employed, working 1:1 or in group sessions in schools and online)
- **Fundraising and Grants Team** (2 people)
- **Marketing and Social Media Manager** (also leads on fundraising events)

All team members use their **personal laptops**, access **GRIT's OneDrive folders**, and handle **sensitive data** via GRIT's **Salesforce CRM**. These tools include names, contact details, session notes, and other personal information of young people.

All safeguarding records are considered sensitive personal data and must be treated with the highest level of confidentiality in line with this policy.

2. **Training Needs Analysis by Role**

Role	Access Level	Training Requirements
CEO	Full access to systems and data	Advanced data protection training, phishing awareness, incident response planning
Chairman and Trustees	Strategic oversight, no direct data	Introductory training on GDPR, information security principles

Operations & Finance Manager	Full access to financial and personal data	Intermediate data protection training, secure file handling, password management
Meetings Coordinator/Admin	Limited data access, calendar/notes	Awareness of confidentiality, email security, handling personal info online
Coaches (10)	Access to personal data, online and in-person delivery	Mandatory GDPR training, secure note-keeping, use of GRIT systems, confidentiality
Fundraising and Grants Team (2)	Access to contact info, CRM data	GDPR and donor data protection, cyber hygiene, secure handling of supporter records
Marketing & Social Media Manager	Access to communication systems and fundraising tools	Social media security, GDPR in marketing, data protection for media and consents, donor data safety

3. Core Training Topics for All Staff

All staff and associates are required to complete annual training and refreshers, with mid-year updates for roles with higher-risk access (e.g., CEO, Operations & Finance Manager). Training may be delivered online or in person. Training will cover:

- Data Protection (GDPR compliance)
- Recognising and reporting phishing and cyber threats
- Secure password creation and management
- Safe use of GRIT's Salesforce system and OneDrive
- Handling sensitive personal data (especially safeguarding-related)
- Procedures for reporting data breaches
- Avoiding use of unsecured public Wi-Fi for confidential work
- Secure disposal of documents and digital files

4. Specialist Training Requirements

- **CEO & Operations Manager** will receive additional training on data breach response and coordination with external regulators (e.g., ICO).
- **Coaches** will receive guidance tailored to mobile work environments, including:
  - Secure notetaking and device locking
  - Avoiding discussing sensitive data in public areas
  - Using video conferencing securely
- **Marketing & Fundraising Roles** will be trained on:
  - Digital privacy rights and marketing GDPR compliance
  - Safe use of social media platforms and securing public event data
  - Handling donor data securely during fundraising activities

5. Tools and Safeguards

GRIT requires all team members to:

- Use two-factor authentication (2FA) for Salesforce and OneDrive
- Store GRIT documents only in designated OneDrive folders (no local device storage)
- Encrypt or password-protect any documents that must be downloaded temporarily
- Ensure devices used for GRIT work have up-to-date antivirus software and firewalls

- Ensure devices auto-lock after periods of inactivity
- Prevent family or other individuals from accessing devices used for GRIT work (no shared accounts)
- Keep operating systems and applications updated with the latest security patches (if applicable)

6. Monitoring and Compliance

- Compliance with this policy is overseen by the **Operations & Finance Manager**
- All suspected or actual breaches must be reported immediately to the CEO and Operations & Finance Manager.
- Training records will be maintained and reviewed annually
- Spot checks or audits may be carried out on adherence to data security protocols
- Any breaches of this policy may result in termination of GRIT access and further investigation under safeguarding or contract management procedures

7. Review and Feedback

This policy and the associated training requirements will be reviewed **annually**, or earlier if…

- There is a change in legislation (e.g., updates to UK GDPR)
- A data breach or cyber incident occurs
- System or software changes are introduced (e.g., changes to CRM or file storage)

Feedback on the effectiveness or clarity of training is welcomed from all GRIT team members.

8. Related Policies and Documents

This policy should be read in conjunction with:

- GRIT Safeguarding Policy
- GRIT Confidentiality Policy
- GRIT Code of Conduct
- GRIT IT Acceptable Use Guidelines
- GRIT Data Protection Statement

- Created by Lydia Casey (Meetings Coordinator/Administrator) on 13/7/25
- Approved by Dr Louise Randall, Chairman

Signature: Date:

_____

- Next review date: 1/7/26