Lower Earley *Family Contact Centre*

# Information Security and Data Protection Policy

## Introduction

This information security policy is a key component of the Lower Earley Family Contact Centre (LEFCC) management framework. It sets the requirements and responsibilities for maintaining the security of information held by LEFCC. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

## Purpose

This policy is intended to support LEFCC objectives and, without undue restrictions, protect its volunteers, clients, third parties and the centre from illegal or damaging events or actions by individuals, either knowingly or unknowingly.
The objective of this policy is to define the LEFCC's policies to protect the confidentiality, integrity and availability of LEFCC's information assets; that is all information held for LEFCC purposes.
Everyone who volunteers for the centre has a duty and a responsibility to comply with these policies.

## Applicability

The policy applies to the use of all IT equipment used for LEFCC purposes, whether owned by the centre or by volunteers (known hereafter as LEFCC IT assets). These may include, but are not limited to: desktops computers, laptops, mobile devices (such as smart-phones) and, removable media.
All volunteers who use LEFCC IT assets shall comply with the information security policy and must understand their responsibilities to protect the Centre's data.

Volunteers have the responsibility to read and understand this policy, and to conduct activities in full accordance with it. If there is any uncertainty, volunteers should consult the Centre Co-ordinator.

## Aim and scope of this policy

The aims of this policy are to set out the rules governing the secure management of our LEFCC information by:

- preserving the **confidentiality, integrity and availability** of our information assets
- ensuring that all volunteers are aware of their responsibilities under this policy
- ensuring an approach to security in which all volunteers fully understand their own **responsibilities**
- creating and maintaining within the organisation a level of **awareness** of the need for information security
- detailing how to **protect** the information assets under our control

This policy applies to all information/data, and the equipment where it is held and all volunteers who have access to the data.

## Responsibilities

### LEFCC

Ultimate responsibility for information security rests with the centre management committee, who are responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy, the business Information Risk Register (including the written risk management measures) is held by the Centre Management Committee, who will review them every two years.

In order to ensure compliance, LEFCC will ensure that all volunteers are aware of this policy and able to understand the threats likely to compromise the information.

**Centre Co-ordinator**
Co-ordinators are responsible for ensuring that their volunteers know:

- Their personal responsibilities for information security
- How to access advice on information security matters

**Volunteer**

- Each volunteer shall be responsible for the operational security of the LEFCC IT assets they use and will comply with the security requirements that are currently in force.
- Each volunteer shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

### Access management

Identity and passwords

- Passwords on any LEFCC IT assets must offer an adequate level of security to protect systems and data
- All passwords shall be eight characters or longer and contain at least two of the following: upper case letters, lower-case letters and numbers

### Risk assessment and management

The LEFCC maintains an information risk register recording any specific vulnerabilities or security risks, the control measures taken to mitigate these risks, and any adjustments over time following changes to the threat environment. It includes:

- A statement of the IT assets deployed by the LEFCC – the asset register.
- A statement of the threats faced by the LEFCC
- A statement of the impacts of compromise of the information assets
- A statement of the tolerable level of risk (the risk appetite)

### Legislation

1. LEFCC is established as an unincorporated association.
2. LEFCC is required to abide by certain UK and international legislation.
3. In particular, LEFCC is required to comply with:
    - The Data Protection Act (2018) (Including GDPR)
    - The Data Protection (Processing of Sensitive Personal Data) Order 2000
    - The Copyright, Designs and Patents Act (1988)
    - The Computer Misuse Act (1990)
    - The Health and Safety at Work Act (1974)
    - Human Rights Act (1998)
    - Freedom of Information Act 2000

### IT asset management

**Intellectual Property rights**

- LEFCC shall ensure that all software held on LEFCC owned IT assets is properly licensed and approved by the coordinator.
- LEFCC does not accept responsibility or liability for the software used on volunteer IT systems that may be used for LEFCC purposes.

**Software management**

- All application software, operating systems and firmware on LEFCC IT assets shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.

**Protection from malicious software**

- All LEFCC owned IT assets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- All anti-malware software shall be set to:
  - scan files on-access
  - automatically check for, daily, virus definitions and updates to the software itself and install new versions when they become available
  - block access to malicious websites.

**Information security incidents**

- All breaches of this policy and all other information security incidents shall be reported to the Centre Co-ordinator.
- All other information security incidents shall follow an SIR (Security Incident Response) procedure which requires:
  - If required as a result of an incident, data will be isolated to facilitate forensic examination.
  - Information security incidents shall be recorded in the Security Incident Log.
  - The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.
- LEFCC has policies, procedures and controls to ensure information assets are identified, valued, handled, stored, processed, transmitted, shared and destroyed in accordance with legal requirements.
- LEFCC will manage the risks associated with digital continuity and records management in respect of all data held electronically, particularly in the event of upgrades in technology, transferral of data into archives and the overall life cycle of data.

**Data Protection**

All client personal information is only accessible to the Centre Co-ordinator.  All such information assets will be managed by the Centre Co-ordinator. No Client PII (Personally Identifiable Information) will be held on removable media.
As the Centre only owns and manages the Co-ordinator mobile phone, there is no need to audit any other information assets or ICT systems to check compliance or extract data in the event of an incident.

All other aspects of Data Protection are covered in the Privacy Policy.