Cumbria Family Support Ltd

INFORMATION SECURITY POLICY

Cumbria Family Support,
The Office,
Mardale Road,
Penrith,
CA11 9EH

Tel: 01768 593102
www.cumbriafamilysupport.org.uk

Statement

Cumbria Family Support (CFS) has a duty under law to ensure that appropriate security measures are taken against unlawful or unauthorised process of personal data, and against the loss of or damage to personal data.

The purpose of the information security policy is to ensure the effective establishment and maintenance of information, information systems, applications and networks preserving the confidentiality, integrity and availability of information.

This policy provides a framework within which to handle information and data in the most secure way.

Security is everyone's responsibility and all CFS employees must make every effort to comply with this policy.

This policy should be read in conjunction with the Confidentiality and Information Sharing Policy.

Scope

The Policy applies to all information whether spoken, written, printed or computer-based, which is held or used by CFS.

The Policy also applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

Objectives

The objectives of the Policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss;
- Information is authentic;
- Information and equipment are protected from accidental or malicious damage;
- Security risks are properly identified, assessed, recorded and managed;
- Safeguards to reduce risks are implemented at an acceptable cost;
- Audit records on the use of information are created and maintained as necessary;
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

Legislation

CFS is obliged to abide by all relevant UK and European Union legislation. All employees must be aware that there are legal requirements relating to information that must be met. Information that relates to individuals is subject to the **Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2018** which places obligations on those who record and use personal data and the organisation for whom they work. CFS is registered with the Office of the Data Protection Registrar. Breaches of the legislation can result in prosecution of both the organisation and individual employees responsible for the breach.

Security Controls

Security education and training will be provided to all employees as appropriate to their assessed needs.

- **Access.** Offices are all designated secure areas. Visitors are to be escorted at all times.
- External doors to be kept locked and locks changed when necessitated.
- Desks and cupboards should be kept locked if they hold confidential information of any kind.
- Confidential files must be kept under lock and key when not being used.
- Confidential files and/or associated papers may only be taken out of the office if absolutely necessary. You are responsible for the safety and security of the information that you take out the office. The information must not be left in view and/or insecure in your car, or on public transport, and at home should be stored securely**.**
- All employees should ensure that they are logged off their computer when the computer is left unattended.
- **Access Categories.** Access to IT will be restricted according to the type of user. Authorised users may only use their account to which they are specifically authorised
- **Equipment Security.** All hardware and software assets held by CFS are to be held against a hardware register and be uniquely marked as being the property of CFS.
- No alteration to the hardware configuration of the system may take place without the permission of the Chief Officer. Under no circumstances are modems to be attached to any part of the system.
- Only approved engineers will be allowed access to hardware and software.

Internal Security

All employees will be fully accountable for the protection of the information they hold and will be responsible for:

- Assessing the risks to the security of the information and the impact of its loss;
- Employing suitable measures to reduce risks;
- Ensuring that equipment is only used for CFS business;
- Ensuring that information is authentic, correct, complete and accurate;
- Ensuring that information exchange with external organisations to or from CFS does not compromise the confidentiality of sensitive information, nor does it increase the risk of data corruption. management:
- All users will have an individual user name for logon.
- **Passwords.** Passwords are an effective security measure only if they are properly constructed and kept secret. Employees must follow the following routines for password
    - Passwords should be given 'values that are not associated with personal characteristics (e.g. children's names, telephone numbers, car registration numbers etc.) Simple and obvious strings of characters and numbers should not be used. It is recommended that a combination of alphabetical, numeric, upper and lower case and system characters are used.
    - Passwords should not be given to anyone else.
    - Passwords should not be written down except as a possible reference, under strict security control.
    - Passwords are not to be used or shared by other users.
    - Users are to change their password at any time that they feel their password has been compromised.

- **Information Exchange.** The exchange of information with and between other organisations and members shall take place within formal arrangements that reflect the legal requirements and the sensitivity of the information. All sensitive information sent by email must be sent via Egress switch.
- **Encryption.** All laptops and mobile phones must have encryption software installed.
- **Housekeeping.** Data is stored on Office 365. All sensitive data should be stored on Office 365 and not on computer desktops.
- Removable storage such as pen drives must be password protected and not used to store sensitive or personal data.
- All software must be licensed and networked applications may be subject to a limited number of users. The Office Manager is to ensure that software is correctly used against licenses held.
- Software is not to be loaded onto any system or PC without the express authority of the Chief Officer.
- **Mobile Computing.** The danger to information stored on portable computers (laptops, notebooks, tablets and smart phones) is recognised. CFS email communication must ONLY be carried out using CFS approved equipment, all of which will have been encryption software installed.
- **Email.** E-mail is not a totally secure system of communication. All confidential emails and attachments must be sent via the Egress switch.
- Normal practice is to use the CFS case number, rather than the clients name within all e-mail correspondence. Names should be replaced with initials.
- **Service Continuity Planning.** Disaster Recovery and Service Continuity plans are in place.
- **Archiving.** Paper files are archived and stored in secure cabinets in a locked room.
- CFS is working towards becoming a paper free organisation and documents are scanned into our electronic case recording systems.
- **Disposal.** The disposal of any information is subject to specific security control.
- Disposal of computer files and disposal of hardware must be under the direction of the IT Service Contract.
- All confidential paper files must be shredded to the minimum of security 3 level.

External Security

- Only employed staff members are authorised to use CFS IT.
- All hardcopies of case file notes and any associated correspondence/reports must be kept securely filed and locked.
- Volunteers must not hold hardcopies of contact sheets and delete electronic copies from their computers when they have been emailed to CFS.

Security incidents and reporting

A security incident is defined as any event that could result or has resulted in:

- The disclosure of unauthorised information to any unauthorised individual;
- The integrity of the system or data being put at risk;
- The availability of the system or information being put at risk;
- An adverse impact, for example:
    - reputational damage to CFS;
    - threat to personal safety or privacy;
    - legal obligation or penalty;
    - financial loss;
    - disruption of activities.

All incidents or information indicating a suspected breach of security must be reported immediately to the Chief Officer.

A record of incidences will be maintained by the Chief Officer.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it;
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on Office 365 and not on individual desktops.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported;
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential);
- **Methods of disposal.** Paper documents should be shredded. Hardware should be destroyed in compliance with the law and relevant certificates received;
- **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

I have read and understood CFS Information Security Policy and agree to abide by the requirements laid down in the Policy.

Name ……

Signature ……

Date ……