



Families Growing Together
Data Breach and Information Security Incident Reporting
Policy and Procedure

Introduction

I hold and process data and information about individuals. I have legal and moral responsibility for protecting this information so that the rights and freedoms of individuals are upheld. When handling information due care and attention will be taken to protect the integrity and security of data about individuals. In the event of a data breach or any other information security incident, appropriate action will be taken to actively manage the situation so as to minimise the impact.

Scope

This Policy and Procedure should be read in conjunction with GDPR Policy and Confidentiality and Privacy Policy.

Policy

This document sets out the procedure that is to be followed upon any data breach or information security incident.

I am responsible for complying with this Policy and reporting any data protection breach or information security incident in accordance with the terms of this Procedure.

I am responsible for any breach of Data Protection brought about by me

Responding promptly and effectively to data breaches and information security incidents ensures compliance with Policy obligations. An early, coordinated and well resourced response to an information security incident can minimise its impact.

Adherence to this Procedure will ensure my response to and management of breaches and incidents is consistent and effective.

Information Security Incident

An information security incident causes or may cause the loss, damage, non availability or unauthorised disclosure of client information, or personal information

The following are examples of incidents:

- Loss of paper records
- Loss of equipment e.g. mobile phone, laptop, iPad or USB stick
- Unauthorised or accidental use, access to or modification of data or information systems (e.g. sharing of user login details (deliberately or accidentally))
- Disclosure of sensitive or personal information (e.g. email or document sent to an unintended recipient or posted in the public domain)
- Loss, damage or destruction of personal data (changes or deletions of documents stored on my systems);
- Disturbance of IT systems resulting in data being unavailable;
- Account being compromised (e.g. via sharing log in details or phishing email);
- Cyber-attack which compromises the security of systems



Procedure following a data breach/information incident

Reporting and Investigation

If I cause or become aware of a data breach, a possible breach or a “near miss” I am required to;

- report this immediately to my team of social work peers.
- Remedial action must be taken promptly. The affected individual will be notified as soon as possible
- All incidents will be investigated in order to establish the nature of the incident, what data and information has been affected, its risk category and the consequences. Investigation will commence as soon as reasonably practicable.
- The investigation will be concluded with a determination of whether the matter needs to be reported to the Information Commissioner’s Office.
- Where, in the opinion of the Data Controllers, it is considered likely that the rights and freedoms of an individual are at risk as a result of a personal data breach, they will notify the Information Commissioner’s Office no later than 72 hours following discovery of the breach.
- Following the investigation of an incident, I will conduct a review and make recommendations.
- Recommendations will be acted on without delay involving changing systems and updating procedures

Enforcement

The ICO has a range of corrective powers and sanctions to enforce GDPR including rectifying data or fines

Responsibilities

I will maintain a register of incidents, regardless of whether they have been reported to the ICO including any investigations carried out and actions taken.

Responsibility for Policy Heidi Pannell

Policy Operational Date 1.2.24

Policy review date 2.8.27