Data Breach Notification Policy

Date approved by the Connected Together CIC Board	24th March 2020
Author/Responsible Person	Michelle Wright
Next revision due	March 2023
Staff/volunteer training delivered	This will be included in staff induction
Date sent to staff	
	This policy covers Connected Together CIC and *all* its contracts and managed organisations, for example Healthwatch North Northamptonshire and West Northamptonshire (HWNW) and Healthwatch Rutland (HWR).
Checked for rebranding	Michelle Wright – 27/04/2022
Signed off by CEO	Kate Holt – 29/04/2022
Checked By	Catherine Maryon (CTCIC Director) - date

1. Introduction

This policy provides further detail to supplement the Connected Together CIC Data Protection Policy.

2. Aim

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

3. Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

a) access by an unauthorised third party.
b) deliberate or accidental action (or inaction) by a data controller or data processor.
c) sending personal data to an incorrect recipient.
d) computing devices containing personal data being lost or stolen.
e) alteration of personal data without permission.
f) loss of availability of personal data.

4. Investigation into suspected breach

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will normally be carried out by the Connected Together CIC (CTCIC) Chief Executive, or his or her nominated deputy, with support of the CTCIC Data Protection Officer (DPO) providing that none of the foregoing are directly involved in the potential breach. In the event that any of these parties are involved in the potential breach then the matter shall be referred to the CTCIC Board, normally via the CTCIC Board Senior Independent Director, who or which shall convene an appropriate investigation and investigators. The above will decide whether the breach is required to be notified to the Information Commissioner following discussion with the CTCIC Data Protection Officer (DPO) and external independent DPO for Healthwatch contracts. A decision will also be made over whether the breach is such that the individual(s) must also be notified.

5. When a breach will be notified to the Information Commissioner

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach including, where possible:
   i) the categories and approximate number of individuals concerned; and
   ii) the categories and approximate number of personal data records concerned
b) the name and contact details of the person to be contacted where more information can be obtained.
c) a description of the likely consequences of the personal data breach; and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

6. When a breach will be notified to the individual

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details of the person to be contacted where more information can be obtained
c) a description of the likely consequences of the personal data breach and

d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

7. Record of breaches

The company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.

Internal Associated Documents

- GDPR Policy-010