The countryside charity
Sussex

# CPRE Sussex Personal Data Breach Procedures

## 1. Introduction

As an organisation that processes personal data CPRE Sussex must ensure appropriate measures are in place to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The General Data Protection Regulation specifies that all breaches (except those 'unlikely *to result in a risk to the rights and freedoms of natural persons)* should be reported to the Information Commissioner *'without undue delay…not later than 72 hours after having become aware of it'.*

In the event of a data breach or an information security incident, it is therefore vital that appropriate actions are taken to promptly report the breach to the Chair of Trustees who will manage the incident.

## 2. Purpose

This procedure is designed to set out the process that should be followed to ensure a consistent and effective approach is in place for managing a data breach across the organisation and ensure that:

- data breach events are detected, reported and monitored consistently
- incidents are assessed and responded to appropriately
- action is taken to reduce the impact of a breach
- relevant breaches are reported to the Information Commissioner within the 72-hour window
- improvements are made to prevent recurrence
- lessons learnt are communicated to the wider organisation.

## 3. Responsibilities

### 3.1 Trustees

The Trustees have responsibility for ensuring that any privacy risks are managed in accordance with the law.

### 3.2 Staff

All users of information assets across the organisation should familiarise themselves with this procedure, be aware of privacy risks and be vigilant in order to ensure breaches are identified, reported and managed in a timely manner.

We want an open and honest culture where people feel comfortable to report mistakes. Support will be provided to ensure everyone has access to the appropriate skills and training to carry out their role effectively. However gross negligence and intentional violations (including not reporting incidents/mistakes) are taken seriously and will lead to disciplinary action.

## 4. Procedures

### 4.1 Identify a Personal Data Breach/Suspected Personal Data Breach

A personal data breach can happen for a number of reasons, for example:

- loss or theft of data or equipment on which data is stored, or through which it can be accessed
- loss or theft of paper files
- hacking attack
- inappropriate access controls allowing unauthorised/unnecessary access to data
- equipment failure
- human error
- unforeseen circumstances such as a fire or flood.

### 4.2 Reporting an Incident

It is vital that as soon as a Personal Data Breach is identified **or suspected** it is immediately reported to the Chair of Trustees. In order to improve our understanding of the risks to data and address them before breaches occur we encourage individuals to report 'near misses' (i.e. incidents which have almost resulted in a data breach except for an intervention or good fortune). Near misses should be reported using the same form and procedure as an actual breach highlighting clearly that the incident is a near miss.

As much information as is immediately available should be collated and then emailed to the Chair of Trustees as soon as possible and within twelve hours of the breach being identified at the very latest, who will then analyse the situation and ascertain whether any immediate corrective/containment/escalation actions are required.

### 4.3 Investigating an Incident

Depending on the type and severity of the incident the Chair of Trustees will assess whether a full investigation into the breach is required. Where required the Chair of Trustees will appoint an appropriate investigation team, who may be external to the organisation who will complete a full breach report.

The investigation will:

a. establish the nature of the incident, the type and volume of data involved and the identity of the data subjects
b. consider the extent of a breach and the sensitivity of the data involved
c. perform a risk assessment

d. identify actions the organisation needs to take to contain the breach and recover information
e. assess the ongoing risk and actions required to prevent a recurrence of the incident.

4.4 Reporting Breach to the Information Commissioner and/or Data Subject

The Chair of Trustees will co-ordinate breach reporting to the Information Commissioner within 72 hours of becoming aware of a relevant breach. He will also evaluate whether the breach is '*likely to result in a high risk to the rights and freedoms*' of the data subject. If this is determined to be the case the incident it will also be reportable to the data subjects without undue delay.

4.5 Escalation

If a breach incident is such that it is considered a serious breach the Chair of Trustees may immediately report the incident to the other Trustees and it may also be necessary to notify the Charity Commission under the Serious Incident Reporting Policy.

Definitions

| | |
|---|---|
| **Personal Data** | 'personal data' means any information relating to an identified or identifiable person ('data subject').<br>An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person; |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. |
| **Special Category Data** | Data which requires extra care and precautions to be taken in its processing and which details or consists of:<br>a. the racial or ethnic origin of the subject<br>b. their political opinions<br>c. their religious or philosophical beliefs<br>d. whether they are a member of a trade union<br>e. processing of genetic data<br>f. processing of biometric data<br>g. data concerning health<br>h. their sexual life/sexual orientation. |

| | |
|---|---|
| **GDPR** | General Data Protection Regulation - a regulation by the European Union intended to strengthen and unify data protection for individuals. It came into force in the UK on 25 May 2018. |