Personal Data Breach Procedures

Contents

Personal Data Breach Procedures

1. Introduction

As an organisation that processes personal data Shropshire Peer Counselling & Advocacy Service (PCAS) 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 '*unlikley 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 Data Protection Team who will manage the incident and minimise associated risks.

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 of the organisation have responsibility to the Clients and Staff for ensuring that any privacy risks are managed.

3.2 All 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.

At Shropshire Peer Counselling & Advocacy Service 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

The Personal Data Breach Reporting Process is represented graphically in Appendix A.

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 Data Protection Officer (Simon Arthur). In order to improve our understanding of the risks to data and address them before breaches occur we would also encourage individuals to report 'near misses' (i.e. incidents which have almost resulted in a data breach except for an intervention or 'luck'). Near misses should be reported using the same form and process as an actual breach highlighting clearly that the incident is a near miss. The General Data Protection Regulation requires that all relevant breaches are reported to the supervisory authority (the Information Commissioner) '*without undue delay….., **not later than 72 hours** after having become aware of it'.*

As much information as is immediately available should be collated and the Personal Data Breach Notification Form (Appendix B) should be completed and emailed to simon@shropshirepcas.co.uk as soon as possible and within twelve hours of the breach being identified at the very latest.

The Data Protection Officer will analyse the form, update the Personal Data Breach Log 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 Data Protection Officer will assess whether a full investigation into the breach is required. Where required the Data Protection Officer will appoint an appropriate investigation team 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 prevent a recurrence of the incident.

4.4. Reporting Breach to the Information Commissioner or Data Subject

The Data Protection Officer will co-ordinate breach reporting to the Information Commissioner within 72 hours of becoming aware of a relevant breach. They 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 will also be reportable to the data subjects without undue delay. Any such report will be coordinated by the Data Protection Officer, assistance will be required from other members of staff.

4.5. Escalation

The Personal Data Breach Log will be reviewed on a regular basis by the Board of trustees who will determine whether any updates to Policy and Procedures are required, and co-ordinate any training and communications messages from the lessons learnt.

If a Breach Report Form is received that outlines a serious breach the Data Protection Officer may immediately escalate the incident directly to the Trustee Board as required, it may also be necessary to notify the Charity Commission under the Serious Incident Reporting Policy.

5. Associated documents and policies

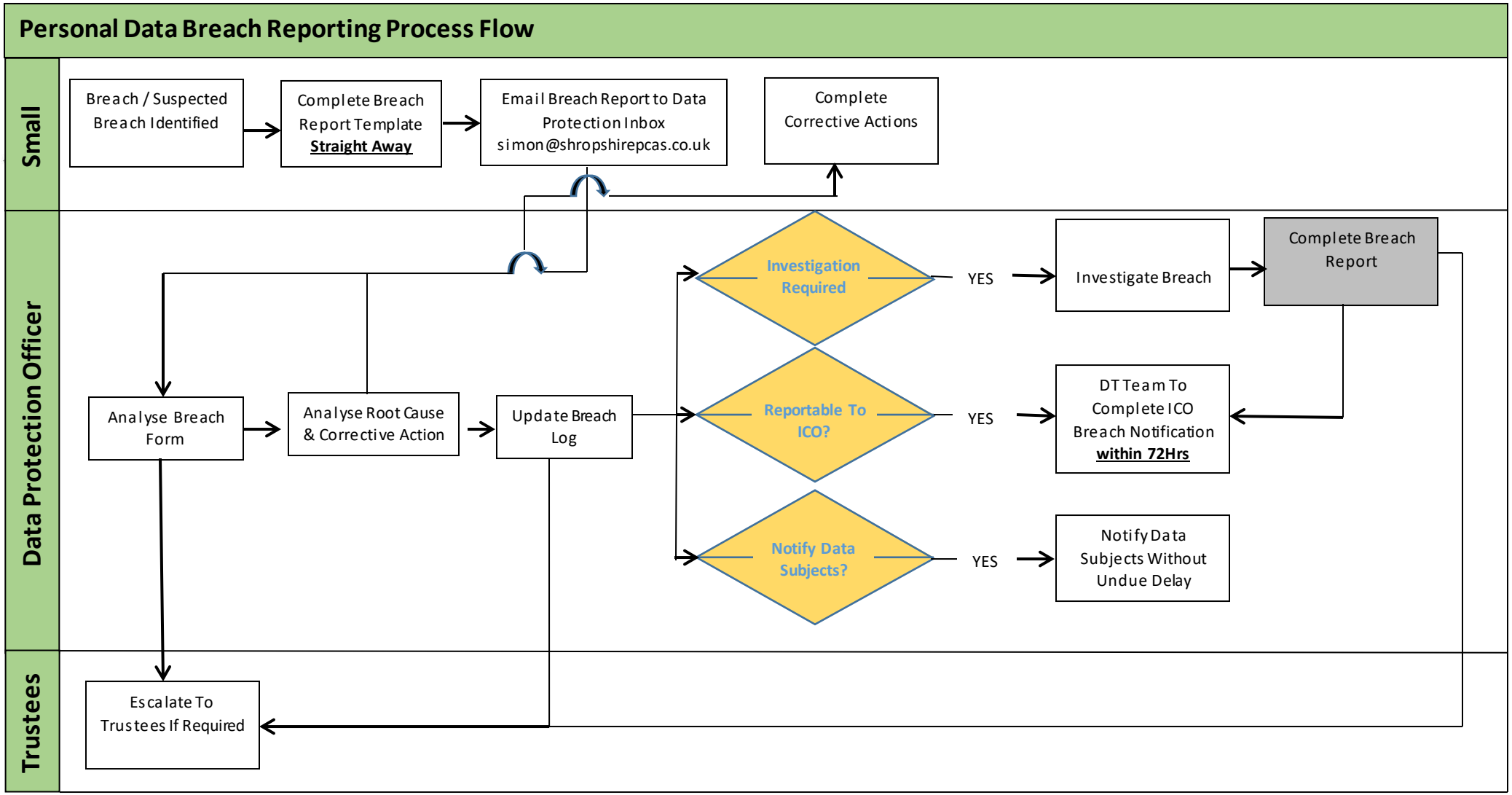
This policy is to be read in conjunction with the related policies;

- Information and Data Retention Policy
- Information and Data Retention Procedure
- Data Protection Policy

6. Definitions

Personal Data	'personal data' means any information relating to an identified or identifiable person ('data subject'). 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; a. the racial or ethnic origin of the subject b. their religious or philosophical beliefs c. data concerning health d. their sexual life/sexual orientation
GDPR	General Data Protection Regulation - a regulation by the European Parliament intended to strengthen and unify data protection for individuals. It comes into force in the UK on 25 May 2018

Appendix A – Personal Data Breach Process



Appendix B – Personal Data Breach Notification Form

Personal Data Breach/Suspected Breach Notification Form	Breach Status			PCAS Here when you need us
	Actual	Suspected	Near Miss	

This form provides a means of reporting all data breaches/suspected breaches and near misses for PCAS
Under GDPR (General Data Protection Regulation) the notification of any data breaches involving personal data have to be made to the Information Commissioner (ICO) within 72 hours of PCAS becoming aware (where a breach is likely to result in a risk to the rights and freedoms of natural persons.
Failure to notify a breach when required to do so can result in a significant fine of up to 10 million euros or 2% of annual turnover. It is therefore essential that all breaches are reported as soon as they occur.
Fill in as much as possible and return ASAP by email to: simon@shropshirepcas.co.uk

Date of Breach	Time of Breach	Overview	How Discovered	Person Reporting Name	No of Records	People Affected	Systems/Databases/Applications Involved	Type of Data/data fields	Special category Y/N	Root Cause	Action Taken