Approved: Oct 2024
Review: Oct 2025

Pontypool Community Council
Cyngor Cymuned Pont-Y-Pŵl

DATA BREACH NOTIFICATION POLICY

1 AIM

1.1 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.

1.2 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.

2 PERSONAL DATA BREACH

2.1 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.

2.2 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.

3 BREACH DETECTION MEASURES

3.1 Examples of ways that data breach may occur and methods used to prevent them used at Pontypool Community Council in liaison with CCSW.

3.2 Failure to have an adequate cyber and physical security system:- control measures are antivirus and firewalls.

3.3 Weak passwords:- Enable two factor authentication.

3.4 Unpatched software:- Patch all software.

3.5 Lack of data encryption:- all of PCC hard drives are encrypted with bitlocker

3.6 Failure to update software:- Patch all software

3.7 Lack of employee cyber threat awareness:- Cyber threat awareness training provided for all staff

3.8 External and internal malicious attacks:- controlled by antivirus and firewalls

3.9 Unsecure web-based applications:- not used at PCC.

3.10 PCC note that detection of a personal data breach is usually detected after the incident, but the control measures above are used to try to mitigate it occurring.

4 INVESTIGATION INTO SUSPECTED BREACH

4.1 In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by The Clerk who will make a decision over whether the breach is required to be notified to the Information Commissioner. 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

5.1 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.

5.2 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.

5.3 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 appointed Compliance Officer 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

6.1 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.

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

6.3 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 appointed Compliance Officer 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

7.1 The Council 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.