Version No.	3
Adopted Date:	October 2024
Last Reviewed Date:	September 2026
Next Review Date:	September 2028

DATA BREACH AND DATA PROTECTION POLICY

1 Introduction and Purpose

1.1 This policy sets out the Council's approach to managing data breaches and data protection.

2 Aim

2.1 We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR), Data Protection Act (2018) as amended by the Data Use and Access Act (2025) in relation to processing data lawfully and to ensure it is kept securely.

2.2 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.

3 Data Breaches

3.1 Personal Data Breach

3.1.1 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.

3.1.2 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.

3.2 Breach Detection Measures

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

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

3.2.3 Weak passwords:- Enable two factor authentication.

3.2.4 Unpatched software:- Patch all software.

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

3.2.6 Failure to update software:- Patch all software.

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

3.2.8 External and internal malicious attacks:- controlled by antivirus and firewalls.

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

3.2.10 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.

3.3 Investigation into a Suspected Breach

3.3.1 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.

3.4 When a breach will be notified to the Information Commissioner

3.4.1 In accordance with the General Data Protection Regulation (GDPR), Data Protection Act (2018) as amended by the Data Use and Access Act (2025), 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.

3.4.2 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.

3.4.3 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.

3.5 <u>When a breach will be notified to the Individual</u>

3..5.1 In accordance with the General Data Protection Regulation (GDPR), Data Protection Act (2018) as amended by the Data Use and Access Act (2025), 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.

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

3.5.3 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.

3.6 Record of Breaches

3.6.1 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.

4 Data Protection

4.1 Personal Data

4.1.1 We may have to collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

4.1.2 We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

4.1.3 To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR), Data Protection Act (2018) as amended by the Data Use and Access Act (2025).

4.1.4 This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.

4.1.5 This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

4.2 Definitions

4.2.1 "Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

4.2.2 "Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

4.2.3 "Criminal offence data" is data which relates to an individual's criminal convictions and offences.

4.2.4 "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.3 Data Protection Principles

4.3.1 Under the General Data Protection Regulation (GDPR), Data Protection Act (2018) as amended by the Data Use and Access Act (2025), all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

a) processing will be fair, lawful and transparent;

b) data be collected for specific, explicit, and legitimate purposes;

c) data collected will be adequate, relevant and limited to what is necessary for the purposes of processing;

d) data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay;

e) data is not kept for longer than is necessary for its given purpose;

f) data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures;

g) we will comply with the relevant GDPR procedures for international transferring of personal data.

4.4 Types of Data Held

4.4.1 We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

4.4.2 Specifically, we hold the following types of data:

a) personal details such as name, address, phone numbers;

b) information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc;

c) details relating to pay administration such as National Insurance numbers, bank account details and tax codes;

d) medical or health information;

e) information relating to your employment with us, including:

- job title and job descriptions
- your salary
- your wider terms and conditions of employment
- details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information

- internal and external training modules undertaken

4.4.3 All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

4.5 Employee Rights

4.5.1 You have the following rights in relation to the personal data we hold on you:

a) the right to be informed about the data we hold on you and what we do with it;

b) the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";

c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';

d) the right to have data deleted in certain circumstances. This is also known as 'erasure';

e) the right to restrict the processing of the data;

f) the right to transfer the data we hold on you to another party. This is also known as 'portability';

g) the right to object to the inclusion of any information;

h) the right to regulate any automated decision-making and profiling of personal data.

4.5.2 More information can be found on each of these rights in our separate policy on employee rights under GDPR.

4.6 Responsibilities

4.6.1 In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

4.6.2 We have also appointed employees with responsibility for reviewing and auditing our data protection systems.

4.7 Lawful Basis of Processing

4.7.1 We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

4.7.2 Where no other lawful basis applies, we may seek to rely on the employee's consent in order to process data.

4.7.3 However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

4.8 Access to Data

4.8.1 As stated above, employees have a right to access the personal data that we hold on them. To exercise this right, employees should make a Subject Access Request. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

4.8.2 No charge will be made for complying with a request unless the request is manifestly unfounded or excessive, or unless a request is made for duplicate copies to be provided to the employee making the request or to a third party acting on the employee's behalf. In these circumstances, a reasonable charge will be applied.

4.8.3 Further information on making a subject access request is contained in our Subject Access Request policy.

4.9 Data Disclosures

4.9.1 The Council may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

b) any employee benefits operated by third parties;

c) disabled individuals - whether any reasonable adjustments are required to assist them at work;

d) individuals' health data - to comply with health and safety or occupational health obligations towards the employee;

e) for Statutory Sick Pay purposes;

f) HR management and administration - to consider how an individual's health affects their ability to do their job;

g) the smooth operation of any employee insurance policies or pension plans;

h) to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

4.9.2 These kinds of disclosures will only be made when strictly necessary for the purpose.

4.10 Data Security

4.10.1 All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.

4.10.2 Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

4.10.3 Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

4.10.4 Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.

4.10.5 Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:

a) ensuring that data is recorded on such devices only where absolutely necessary;

b) using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted;

c) ensuring that laptops or USB drives are not left where they can be stolen.

4.10.6 Failure to follow the Council's rules on data security may be dealt with via the Council's disciplinary procedure, appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

4.11 Third Party Processing

4.11.1 Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the Council's commitment to protecting data.

4.12 International Data Transfers

4.12.1 The Council does not transfer personal data to any recipients outside of the EEA.

4.13 Requirement to Notify Breaches

4.13.1 All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

4.13.2 More information on breach notification is available in our Breach Notification policy.

4.14 Training

4.14.1 New employees must read and understand the policies on data protection as part of their induction.

4.14.2 All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

4.14.3 The nominated data controller/auditors/protection officers for the Council are trained appropriately in their roles under the GDPR.

4.14.4 All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the Council of any potential lapses and breaches of the Council's policies and procedures.

4.15 Records

4.15.1 The Council keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

4.16 Data Protection Compliance

Our Data Protection Officer is:

Name: Cathryn Drew, Clerk
Contact Details: Email: clerk@pontypoolcc.gov.uk
Tel: 01495 365951