

Policy

Data Breach Policy

This Procedure is a document that sets out the organization's approved and agreed practices. Any deviation must be discussed with the originating author.

DOCUMENT NO:	PCD039		
Lead author(s):	Cllr A Catlett		
Developed by:	Cllr. A Catlett		
Approved by:	Full Council		
Ratified by	Full Council		
Ratification date:	13 May 24		
Due Review date:	May 25 (Annual Meeting)		
Version no:	5		
Version Control and Revisions:			
1	First Published		June 2018
Version	Point	Description of change	Date
2	All	Format changes following review	6 March 2021
3		Annual Review. No changes	Jul 2022
4		Annual Review. No changes	May 23
5		Annual Review. Minor format changes.	May 24

THIS IS A CONTROLLED DOCUMENT

Whilst this document may be printed, the electronic version maintained on the Billingham Parish Council website is the controlled copy. Any printed copies of this document are not controlled.

© Billingham Parish Council. Not to be reproduced without written permission.

1. DOCUMENT CONTROL SHEET

Purpose of document:	The purpose of this policy is to remind and inform all staff and council members within Billingham Parish Council of their duties where there is a breach of data
Dissemination:	This policy will be disseminated to all staff and council members and be made available on the parish website
Implementation:	This document will be accessible via the parish council website and is applicable to all staff and council members.
Review:	This document will be reviewed in 2025 at Annual Meeting unless there are significant changes in legislation or practice in which case it will be reviewed earlier.
Documents replaced or superseded by this document:	
This document supports (enter Standards and Legislation):	General Data Protection Regulation (GDPR) (2018)
Key related documents:	PCD0010 Data Protection Policy PCD0040 Records Retention Policy
Financial Implications:	This document has potential implications for the Billingham Parish Council where a data breach occurs
Key word search	Data Breach

2. TABLE OF CONTENTS

1. DOCUMENT CONTROL SHEET	2
2. TABLE OF CONTENTS	3
3. INTRODUCTION	3
4. CONSEQUENCES OF A PERSONAL DATA BREACH	3
5. DUTY TO REPORT A BREACH	3
6. DATA PROCESSORS DUTY TO INFORM THE PARISH COUNCIL	4
7. RECORD OF DATA BREACHES	4
8. APPENDIX 1 – DATA BREACH FORM	5

3. Introduction

a. GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- i. Access by an unauthorised third party.
- ii. Deliberate or accidental action (or inaction) by a controller or processor.
- iii. Sending personal data to an incorrect recipient.
- iv. Computing devices containing personal data being lost or stolen.
- v. Alteration of personal data without permission.
- vi. Loss of availability of personal data.

Billinghay Parish Council (‘the Council’) takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

4. Consequences of a personal data breach

a. A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

5. Duty to report a breach

b. If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and the Information Commissioner’s Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer (DPO) must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

- b. If the ICO is not informed within 72 hours, the Council via the DPO must give reasons for the delay when they report the breach.
- c. When notifying the ICO of a breach, the Council must:
 - i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
 - ii. Communicate the name and contact details of the DPO.
 - iii. Describe the likely consequences of the breach.
 - iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.
- d. When notifying the individual affected by the breach, the Council must provide the individual with (ii)-(iv) above.
- e. The Council will not need to communicate with an individual if the following applies:
 - i. It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it.
 - ii. It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
 - iii. It would involve a disproportionate effort
- f. However, the ICO must still be informed even if the above measures are in place.

6. Data processors duty to inform the Council

- a. If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify the Council without undue delay. It is then the Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

7. Record of data breaches

- a. All data breaches must be recorded whether they are reported to individuals or not. This record will help to identify system failures and should be used to improve the security of personal data. Data breach form is available in Appendix 1

To report a data breach use the ICO online system:

<https://ico.org.uk/for-organisations/report-a-breach/>

8. Appendix 1 – Data Breach Form

Date of Breach	Type of Breach	Number of Individuals affected	Date reported to ICO / Individual	Actions to prevent breach recurring