WEST Hill Parish Council

Data Breach Policy

ADOPTED WHPC Meeting 3rd February 2026 Min 26/040

1. Introduction

Information is a major asset that West Hill Parish Council has a duty and responsibility to protect.

The processing of personal data is essential to many of the services and functions we carry out. In so doing we recognise the importance of the need to comply with the requirements of the data protection legislation and other relevant legislation which seeks to protect an individual's fundamental rights and freedoms.

This policy relates to Data Breaches. It should be read in conjunction with our "Data Protection Policy" which sets out the measures we have put in place to protect Personal Data (available on our website or on request).

A **'personal data breach'** means 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.

Examples include:

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

As a Data Controller, the Parish Council **MUST** report a personal data breach to the Information Commissioner within 72 hours of becoming aware of the breach - unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where notification is not made within 72 hours, the controller should provide reasons for the delay.

When a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, West Hill Parish Council **MUST** communicate the personal data breach to the data subject without undue delay, unless specific conditions apply. These conditions include the implementation of technical measures, such as encryption which would render the data unintelligible to any person not authorised to access it, taking measures to contain the initial high risk, or it would involve disproportionate effort (in which case a public communication or similar measure can be used to inform data subjects).

If personal data held by the Council is mishandled, the law requires that it respond in certain ways. This document sets out how the Council will meet its legal obligations should such a situation ever arise.

2. Scope

The Data Breach Policy applies to all Councillors, employees of the Council, contractual third parties and agents of the Council who have access to information systems or information used for West Hill Parish Council purposes.

Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video

3. Consequences of a personal data breach

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.

4. West Hill Parish Council duty to report a data breach

4.1. 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 ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

4.2. Who leads the response?

West Hill Parish Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Parish Clerk.

The Parish Clerk must be informed immediately so that they are able to report the breach to the ICO in the 72 hour timeframe. If the ICO is not informed within 72 hours, West Hill Parish Council must give reasons for the delay when they report the breach

4.3. Reporting a Data Breach

To report a data breach use the ICO online system: Report a breach | ICO www.ico.org.uk/for-organisations/report-a-breach/

The ICO provides guidance on the reporting of Data Breaches and provide a Self-assessment tool. www.ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/ . They advise:

- If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. When you've made this assessment, if it's likely there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report. You do not need to report every breach to the ICO.

Take our self-assessment to help determine whether your organisation needs to report to the ICO.

When notifying the ICO of a breach, West Hill Parish Council must:

a. 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.
b. Communicate the name and contact details of the DPO
c. Describe the likely consequences of the breach
d. Describe the measures taken, or proposed to be taken, to address the personal data breach including measures to mitigate its possible adverse effects.

When notifying the individual affected by the breach, the Parish Council must provide the individual with (a)-(d) above. West Hill Parish Council would not need to communicate with an individual if the following applies:

- 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;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

5. Records of data breaches

All data breaches must be recorded, whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/Individual	Actions taken to prevent breach recurring

6. West Hill Data Breach Procedure

If a Data Breach has occurred or may have occurred the following procedure will be followed:

6.1. What is a data breach?

The mishandling of personal data (“a data breach”) can happen in many ways. The following list describes some of the most common (it is not a complete list):

- Sending or copying an email to an unintended recipient. • Copying an email to recipients using “cc” rather than “bcc”;
- Accidental loss or theft of a memory stick, laptop computer, CD-ROM, etc.

- Unauthorised persons gaining access to physical or electronic records (e.g. during a burglary or computer hack).
- Accessing records for no proper purpose (e.g. staff and councillors may need to consult records for a legitimate purpose, but it may be illegal for them to do so out of idle curiosity).
- Improper deletion or alteration of records (including by malicious persons or software);
- Ignoring or mishandling a legitimate request for data to be corrected or deleted.

Sometimes it is obvious when a data breach has happened, but this is not always the case. In case of doubt (that is, if you think that a data breach may have happened but are not necessarily sure) then you must follow this procedure.

6.2. **Who does this procedure apply to?**

- If you work for the Council (whether as an employee, a worker, or a free-lancer or contractor) then this procedure applies to you. Failure to do so without a lawful excuse may result in disciplinary or enforcement action being taken against you. In a sufficiently serious case this could result in dismissal without notice or immediate termination of your contract for services.
- Councillors are also required to conduct themselves in accordance with this procedure. Failure to do so without a lawful excuse or impeding staff in the application of the procedure may amount to a breach of the Code of Conduct.

6.3. **What to do if a data breach is known or suspected**

If you have reason to believe that a data breach has happened or may have happened, you **MUST** complete a Data Breach Report Form (see form below) as this form details the procedure and the appropriate response to the data breach. The form will then be kept confidentially at the Council Office for council records only.

Do not worry if you cannot fill in every part of the form fully – fill in as much as you can. It is important not to delay for any reason – this is more important and urgent than anything else you may have to do (apart from medical emergencies or immediate threats to someone's physical safety)

Send the completed form to the Parish Clerk as soon as you can by email. If this is not possible, deliver hard copies to them in person at the council office.

6.4. **Responding to a Data Breach Report**

- Upon receiving a Data Breach Report Form the Parish Clerk will take responsibility for the subsequent handling of the matter. Where this is not possible responsibility will fall on the Chairman.
- The responsible individual will then invoke and follow the Data Breach Checklist & Action Plan set out below.
- The Parish Clerk will invoke and follow the Data Breach Checklist & Action Plan set out below. (Appendix 1)

6.5. **Reviewing the Data Breach**

The Patrish Council will review the data breach to improve its procedures and security,

Version History

First ADOPTED WHPC Meeting 3rd February 2026 Min 26/040

Appendix 1

WEST HILL PARISH COUNCIL – Data Breach Report form

Details of Breach (Describe briefly what has happened or how the data breach arose with dates and times where possible)	
Nature and content of data involved (Describe the type(s) of personal information involved e.g., email addresses, payroll information, medical information, etc.)	
Number of individuals affected.	
Name of person making this report.	
How and to whom this report was submitted	
Date and time this report was submitted.	
Date and time of Notification of Breach	
Notification of Breach received from Name Contact Details	
Report form attached.	
How and when report acknowledged	
Name of person investigating breach: Name Job Title Contact details Email Phone number Address	
Further information about breach (not contained in report form)	
Information Commissioner informed if relevant Time and method of contact	

https://report.ico.org.uk/security breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted • How many individuals contacted? • Method of contact used to contact. • Does the breach affect individuals in other EU member states? • What are the potential consequences and adverse effects on those individuals? • Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Members briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and Response	