



West Horsley Parish Council

DATA BREACH POLICY

Introduction

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 of data breach incidents 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

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.

Scope of this Policy

West Horsley Parish Council (WHPC) has legal responsibilities to ensure that the information within its control is safeguarded. Care will be taken to protect information, to ensure its integrity and to protect it from loss, theft or unauthorised access.

This policy sets out the procedures WHPC will follow on the reporting of a data breach. It applies to all councillors, committees, employees of the Council, contractual third parties and agents of the Council who have access to information systems or information used for WHPC purposes.

Any member of the above discovering or suspecting a data breach incident must report it in accordance with this policy.

When to report a breach

All data breaches should be reported immediately to the Parish Council via the clerk at clerk@westhorsley-pc.gov.uk. The clerk will require the person reporting the data breach to provide further information, the nature of which will be dependent upon the incident being reported.

For all types of breaches being reported, the following must be supplied:

- Contact details of the person reporting the breach
- Type of data or information involved (not the data unless specifically requested)
- Whether the data related to people and if so, how many
- Location of the incident

- Inventory and location of any equipment affected
- Date and time the data breach occurred
- Type and circumstance of the incident

The Chairman of the Parish Council will also be informed to enable them to investigate and confirm that the details represent a valid data breach as defined above. The Clerk and the Chairman will be responsible for the initial assessment to determine the severity of the breach based on scope, scale and risk.

West Horsley Parish Council's Duty to Report a Breach

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 Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. If the ICO is not informed within 72 hours, WHPC must give reasons for the delay when they report the breach.

When reporting a breach to the ICO WHPC will:

- 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) Provide the name and contact details for WHPC (the clerk)
- 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.

If the breach is likely to result in a high risk to individuals' rights and freedoms, the Parish Council must also inform the individual(s) without undue delay. If the risk is not considered high WHPC does not need to notify the individual(s), however, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. If the Council decides it does not need to report the breach to the ICO, it must document its decision giving its reasons.

Review and Records of Data Breaches

Once an incident has been contained, WHPC will undertake a thorough review of the event to establish the cause of the data breach and the effectiveness of the response, and will identify areas that require improvement. Any recommended changes to systems, policies and procedures will be documented and implemented as soon as possible. Any weakness or vulnerabilities that may have contributed to the incident will be identified and plans put in place to resolve and avoid any future events.

The Parish Council is responsible for maintaining a confidential log of all data breach events, whether or not they are reported to individuals. This record will help to identify system failures and should be used to improve the security of personal data.

To report a data breach to the ICO, go to <https://ico.org.uk/for-organisations/report-a-breach/>.

Policy to be reviewed and adopted by Full Council on 21 July 2026

Next review: July 2028