DRAFT
WEST LAVINGTON PARISH COUNCIL

Data Breach Policy

1. Purpose

West Lavington Parish Council processes and shares personal information in accordance with its Privacy Policies, a valuable asset that needs to be appropriately protected.

Data security breaches can occur for a number of reasons including:

- emails containing personal or sensitive information sent in error to the wrong recipient;
- personal data is held for longer than is required;
- personal data processed without individuals knowledge or consent;
- sensitive personal data is accessed by persons without authority;
- the disclosure of confidential data to unauthorised individuals;
- improper disposal of documents leaving personal data deposited where it can be accessed by the general public;
- loss or theft of data or equipment on which data is kept (e.g. of a laptop, USB stick, iPad/tablet);
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of sensitive/confidential material;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- viruses or other security attacks on equipment systems or networks;
- breaches of physical security;
- confidential information left unlocked in accessible area.

In respect of this policy a breach can be defined as 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.

A personal information/data breach may result in harm to an individual, reputational damage, legislative non-compliance and/or financial fines.

The purpose of this policy is to ensure that a procedure is in place for dealing effectively with any data breach. This policy is compulsory and by accessing any of the Parish Council's information/data, users are agreeing to abide by the terms of the same.

2. Scope

This policy applies to all councillors, staff, volunteers, service providers, contractors, consultants and third parties who access, use, store or process information while working for or on behalf of the Parish Council. This policy is authorised by the Parish Council. It applies to all personal and sensitive information held by the Parish Council in whatever format.

3. Legislation

The Parish Council is obliged to abide by all relevant UK and European data protection legislation.

4. Policy

The objective of this policy is to identify and report any incident of data breach, contain and minimise the associated risk, notify the breach and prevent further breaches.

5. Data Breach Management Plan

5.1 Identification and Reporting

Anyone who accesses, uses or manages the Parish Council's personal information must report data breach or information security incidents immediately to the Clerk at: clerk@westlavington.org.uk. If it occurs or is found outside normal office hours it must be reported as soon as practicable. Details of breaches should be recorded accurately, including:

- the date and time the breach occurred;
- the date and time it was discovered;
- full and accurate description of the breach, including the nature of the personal information;
- who reported the breach;
- details of any ICT systems involved;
- how many individuals are involved;
- any other substantiating material.

5.2 Containment and Recovery

Containment comprises restricting both the scope and impact of the breach.

If a breach occurs:

1. The Clerk will make an initial assessment with the Chair and relevant councillors, including firstly to determine if the breach is still occurring and the severity of the breach.
2. The Chair with relevant councillors will determine who will take the lead investigating the breach (which will depend on the nature of the breach).
3. The lead councillor(s) will then establish who may need to be notified as part of the initial containment (for example, the police) and then whether there is anything that can be done to recoup losses and limit the damage the breach may cause.
4. The lead councillor(s) will determine the suitable course of action to ensure resolution.
5. Details of the facts relating to the breach, its effects and remedial action taken are then entered in the Parish Council's internal breach register.

5.3 Risk Assessment

In assessing the risk arising from the breach, an investigation will be undertaken promptly by the lead councillor(s) who should consider the potential adverse consequences for individuals, for example, how serious and how likely to occur.

In assessing the risk, the investigation will consider the following:

- Nature of information/data involved
- Sensitivity of the information/data
- Any security mechanisms that are in place (e.g. password, encryption)
- What has happened to the data, has it been lost or stolen or destroyed?
- What could the information/data convey to a third party about the individual?
- How many individuals are affected by the breach and the potential effects on those individuals?
- Any wider consequences of the breach.

5.4 Notification of Breach

All information/data breaches must be reported immediately to the Clerk and an incident report must be completed (see Appendix attached), including:

- Date incident was discovered;
- Date(s) of incident;
- Place of incident;
- Name of person reporting incident;
- Contact details of person reporting incident (email address, telephone number);
- Brief description of incident or details of the information lost;
- Number of individuals affected, if known;
- If any personal data has been placed at risk and brief details of same;
- Brief description of any action taken at the time of discovery etc.

The lead councillor(s) will decide who needs to be notified of the breach, such as the police, insurers, bank or credit card companies in the event of potential illegal activity.

The following should be considered:

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected;
- Whether notification would help prevent the unauthorised or unlawful use of personal information;
- Whether notification would help the Parish Council meet its obligations under the seventh data protection principle – which provides that: “appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.

The Information Commissioner’s Office will be notified in accordance with Article 33 of the General Data Protection Regulation without undue delay and, where feasible, not later than 72 hours after having become aware of a data breach (unless the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons). Where the

notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

A notification to the ICO must at least:

- describe the nature of the personal data breach, including the number and categories of individuals and personal data records affected;
- provide contact information;
- describe the likely consequences of the personal data breach; and
- describe proposals to address the breach, including any mitigation efforts.

If not all information is available at once, it may be provided in phases.

If the personal data breach is likely to result in a high risk to the rights and freedoms of an individual, information regarding the personal data breach must be communicated to the affected individual without undue delay in accordance with Article 34 of the General Data Protection Regulation. Notification to individuals whose personal data has been affected will include a description of how and when the breach occurred and the data involved, on what can be done to protect themselves and what steps have been taken to mitigate the risks. The Clerk should be contacted for further information.

5.5 Evaluation and Response

Subsequent to any information/data security breach a thorough review of the event should be undertaken by the lead councillor(s) who will consider:

- Where and how personal data is stored
- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies, procedures or reporting lines need to be amended to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are all councillors, staff and volunteers cognisant of their responsibilities for information security and adequately trained?
- Are methods of transmission secure?
- Is additional investment required to lessen exposure and if so what are the resource implications?

Any recommended changes to policies and/or procedures must be documented and implemented as soon as possible by the Parish Council.

6. Roles and Responsibilities

6.1 Parish Council

The Parish Council is responsible for:

- Implementation of this policy on a day-to-day basis.
- Ensuring that all councillors, staff and volunteers are made aware of and are instructed to comply with this policy.

6.2 Users

Each policy user is responsible for:

- Complying with the terms of this policy and all relevant data protection legislation and applicable legislation; and
- Valuing and protecting the privacy and confidentiality of the information they process at all times.

7. Enforcement

The Parish Council reserves the right to take such action as it deems appropriate against users who breach this policy.

8. Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any relevant and necessary changes are accurately reflected. The date below will indicate when this Privacy Notice was last updated. Any changes are effective from that date.

Adopted May 2018

APPENDIX

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify the Clerk immediately, by completing Section 1 of this form and emailing it to the Clerk at: clerk@westlavington.org.uk.

Section 1: Notification of Data Security Breach	**To be completed by person discovering breach**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of individuals affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Clerk	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Clerk in consultation with the Chair and Lead Councillor/s**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, financial legal, liability or reputational consequences for the Parish Council or third parties?	
How many individuals are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Sensitive personal data** (as defined in the GDPR) relating to a living, identifiable individual(s) a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings. • Information that could be used to commit	
identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; • Personal information relating to vulnerable adults	
and children; • Detailed profiles of individuals including	
information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	

Section 3: **Action taken**	**To be completed by Clerk and/or Lead Councillor/s**
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible Lead Councilor/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to the Clerk , Chair and Lead Councillor /s on (date):	
Reported to Parish Council (details, dates):	

For use of the Clerk and/or Lead Councillor(s):	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**
Notification to affected individual (s)	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/agency/stakeholder	**YES/NO If YES, notified on:** **Details:**