HORNDEAN PARISH COUNCIL
DATA BREACH POLICY

1. Background

Data security breaches are increasingly common and as the amount of data grows, there are new ways by which data can be breached, particularly given the development in technology.

2. Aim

The aim of this policy is to standardise the Council's response to any data breach and ensure that they are appropriately recorded and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operation are restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further incidences
- the ICO (Information Commissioner's Office) and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned.

3. Definition

Article 4 (12) of the General Data Protection Regulation (GDPR) defines a data breach as:

"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Horndean Parish Council (the Council) is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how the Council will manage a report of a suspected data security breach.

The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

A data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy
- Data posted, emailed or faxed to the incorrect recipient

- Loss or theft of equipment on which data is stored
- Inappropriate sharing or dissemination – staff accessing information to which they are not entitled
- Hacking, malware, data corruption
- Information is obtained by deception
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data.

In any situation where staff are uncertain whether an incident constitutes a breach of security, report it to the Data Protection Officer (DPO). In respect of IT issues, such as the security of the network being compromised, the IT provider should be informed immediately.

4. Scope

This policy applies to all Council information, regardless of format, and is applicable to all officers, members, visitors, contractors, partner organisations and data processors acting on behalf of the Council.

5. Responsibilities

Information users

The GDPR applies to both Data Controllers (the Council) and to Data Handlers. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers

Responsible for ensuring that staff act in compliance with this policy and assist with investigations as required.

6. Reporting a Breach

Internal

Suspected data security breaches should be reported promptly to the DPO as the primary point of contact on 02392 597766, email: carla.baverstock-jones@horndeanpc-hants.gov.uk

The report must contain full and accurate details of the incident including who is reporting the incident (and what classification of data is involved). The incident report should be completed as part of the reporting process. See Appendix 1. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach. See Appendix 2. All data security breaches will be recorded by the DPO to ensure appropriate oversight in the types and frequency of confirmed incidents for managing and reporting purposes.

External

Article 33 of the GDPR requires the Council as data controller to notify the ICO only when the breach “is likely to result in a risk to the freedoms and rights of

natural persons". Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made without undue delay and within 72 hours of becoming aware of it. If the Council fails to do this, it must explain the reason for the delay.

Article 33(5) requires that the Council must maintain documentation on data breaches, their nature and remedial action taken.

A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

7. Data Breach Plan of Action

The Council's response to any reported data security breach will involve the following 4 elements:

- Containment and Recovery
- Assessment of Risks
- Consideration of Further Notification
- Evaluation and Response.

An activity log recording the timeline of the incident management should also be completed.

8. Disciplinary

Officers, members, contractors, visitors or partner organisations who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.

9. Review

This document shall be subject to annual review by the DPO/Council.

10. References

- The GDPR
- ICO Guidance on Data Breaches