Information Security Incident Policy

1. POLICY STATEMENT

1.1 Heworth Without Parish Council, hereinafter also referred to as “the Parish Council” or as “ the Council” holds information in a variety of formats stored in computers /books, printed documents and images in the form of photographs. This includes personal and sensitive personal data and non-personal information which may be sensitive or commercially confidential.

1.2 The Parish Council 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.

2. SCOPE OF THE POLICY

2.1 This policy defines an Information Security Incident and sets out the Parish Council's procedures in response to the reporting of an information security incident (also referred to as a ‘data breach’).

The policy covers all types of information - written, spoken and computer information - and where something has occurred which has created an impact on the confidentiality, integrity and availability of that information.

2.2 This Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties, volunteer groups and agents of the Council who have access to Information Systems or information used for Heworth Without Parish Council purposes.

2.3 Any member of the above discovering or suspecting an information security incident must report it in accordance with this policy.

This policy should be read in conjunction with the following policies:

- Data Protection
- Privacy Policy
- Records Management

3. DEFINITION

An information security incident is an event which occurs when data or information held by the Parish Council, in any format, is compromised by being lost, destroyed, altered, copied, stolen, transmitted, unlawfully accessed or used by unauthorised individuals whether accidentally or on purpose.

4. WHAT IS COVERED BY AN INFORMATION SECURITY INCIDENT?

- The loss or theft of data or information
- The loss or theft of equipment upon which the data is stored

• Unauthorised access to data or information storage or computer systems/ Introduction of unauthorised or untested software

Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system

• Transfer of data or information to those who are not entitled to receive that information/ Information leakage due to software errors.

• Failure of equipment or power leading to loss of data / Deterioration of backup tapes

• Environmental – deterioration of paper records /Damage caused by natural disasters e.g. fire, burst pipes, lighting etc

Loss of integrity of the data within systems and transferred between systems

• Changes to information or data or system hardware, firmware or software characteristics without the council's knowledge, instruction or consent

• Unauthorised use of a system for the processing or storage of data

• Data maliciously obtained by way of social engineering (i.e. an attack in which a user is 'tricked' into giving third-party access)

5 WHEN TO REPORT THE BREACH

5.1 All information security breaches should be reported immediately to the Parish Council via the Clerk to the Council.

5.2 The Clerk to the Council will require the person reporting the security incident to provide further information, the nature of which will be dependent upon the incident being reported.

5.3 In all types of breaches being reported the following must be supplied:

• Contact details of the person reporting the breach

• The type of data or information involved (not the data unless specifically requested)

• Whether the data related to people and if so how many people were involved

• Location of the incident

• Inventory and location of any equipment affected

• Date and time the security incident occurred

• Type and circumstances of the incident.

5.4 The Chair of the Parish Council will also be informed to enable him/her to investigate and confirm that the details represent a security incident as defined above.

5.5 Should the data breach be caused or realised by the Clerk of the Council, he/she must immediately report it to the Chair and Vice-Chair (if any) of the Council and follow all stages detailed in 5.3 and 5.5.

5.6 The Parish Council is responsible for maintaining a confidential log of all information security events.

6 INVESTIGATION AND RESPONSE

6.1 The Parish Council will consider the report, and where appropriate, require the Policy & Resources Committee to be responsible for investigating the circumstances and the effect(s) of the information security incident.

6.2 An investigation will be started into material breaches within 24 hours of the breach being discovered, where practicable.

6.3 The investigation will cover the nature of the incident, the type of data involved, whether the data is personal data relating to individuals or otherwise confidential or valuable. If personal data is involved, associated individuals must be identified and, if confidential or valuable data is concerned, the legal and commercial consequences of the breach should be assessed.

6.4 The investigation will cover the extent of the sensitivity of the data and a risk assessment will be carried out as to what might be the consequences of the loss. This will include damage and / or distress to individuals and the Parish Council.

6.5 The Policy and Resources Committee will be responsible for formally recording the incident and the associated response. This report will be subject to review by the Parish Council.

7 ESCALATION & NOTIFICATION

7.1 The Employment Committee will be responsible for the initial assessment of an incident's severity based on scope, scale and risk of the incident.

7.2 The preliminary decision is then to be reviewed by the full Parish Council.

7.3 If a serious personal data breach has occurred the Parish Council will instruct the Parish Clerk as the Proper Officer of the Council to notify the Information Commissioner's Office (ICO) within the prescribed statutory limits and the Parish Clerk will manage all communications between the Parish Council and the ICO.

7.4 If the breach is deemed to be of sufficient seriousness (in line with ICO guidance) and concerns personal data, notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. Such a notice will include a description of the breach and the steps taken by the parish council to mitigate the risks and will be carried out by the Employment Committee. Liaison with the Police and other authorities may be required for serious events.

8 REVIEW

8.1 Once the incident has been contained, the Employment Committee will undertake a thorough review of the event to establish the cause of the incident, the effectiveness of the response and will identify the areas that require improvement.

8.2 Any recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

8.3 Any weaknesses or vulnerabilities that may have contributed to the incident will be identified, reported at a full Parish Council meeting and plans put in place to resolve and avoid any future incidents occurring.

The Policy will be reviewed annually.
Adopted in December 2021 Review date December 2022