Scarning Parish Council
Information Security Incident Procedure

1 Introduction

Scarning Parish Council holds information in a variety of formats, including computers and printed documents. The Council holds personal data as well as non-personal information, which may be sensitive or commercially confidential.

The Parish Council has a legal responsibility to ensure that the information within its control is safeguarded. Care is taken to protect information, to ensure its integrity and to protect it from loss, theft or unauthorised access.

This Procedure defines an Information Security Incident and sets out the procedure to be followed on the reporting of an Information Security Incident (also referred to as a data breach).

This document applies to councillors, Council employees , contractors and agents of the Parish Council who have access to information systems or information used by the Parish Council.

Any member of the above discovering or suspecting an Information Security Incident must report it in accordance with this policy.

2 An Information Security Incident

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

3 What is Covered by an Information Security Incident

- The loss or theft of data/information
- The loss or theft of equipment on which data is stored
- Unauthorised access to data/information storage or computer systems
- Transfer of data/information to those who are not entitled to receive that information
- Failure of equipment or power leading to loss of data
- Deterioration of paper records
- Changes to information/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 (ie an attack in which a user is tricked into giving a third party access).

4 When to report a Breach

4.1 All Information Security Incidents should be immediately reported to the Clerk.

4.2 The Clerk will require the person reporting the incident to provide further information, the nature of which will be dependent on the incident being reported.

4.3 In all types of breaches the following must be supplied:-

- Contact details of the person reporting the breach
- The type of data/information involved
- Whether the data is related to people and if so how many people involved
- Location of the Incident
- Inventory and location of any equipment affected
- Date and time the Security Incident occurred
- Type and circumstance of the Incident

4.4 The Council Chair will be informed to enable them to investigate and confirm that the details represent a valid security incident as defined above.

5 Investigation and Response

5.1 The Council will consider the report and will be responsible for investigating the circumstances and the effect of the Information Security Incident.

5.2 Where practical, an investigation into material breaches will commence within 24 hours of the breach being discovered.

5.3 The investigation will cover the nature of the incident, the type of data involved, whether the data is personal data referring 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, what the legal and commercial consequences of the breach may be.

5.4 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 consequence of the loss. This will include damage and/or distress to individuals and the Parish Council.

5.5 The Council will be responsible for preparing a report which formally records the incident and the associated response.

6 Escalation and Notification

6.1 The Council is responsible for the individual assessments of the severity of an Incident based on scope, scale and risk.

6.2 If a personal data breach has occurred on a significant scale the Council will instruct the Clerk to notify the Information Commissioner's Office within the prescribed statutory limits.

The Clerk will manage all communications between the Parish Council and the Information Commissioner's Office.

6.3 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 in conjunction all relevant authorities.

7 Review

7.1 Once the incident has been contained, the Council will undertake a thorough review of the Incident to establish its cause and the effectiveness of the response. The review will seek to identify any areas requiring improvement.

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

7.3 Any weaknesses or vulnerabilities that may have contributed to the incident will be identified and reported to the full Council. The Council will put in place plans to resolve and avoid the occurrence of any future incidents.

Approved: February 2024.
Next review: February 2025.