DENHAM PARISH COUNCIL

INFORMATION SECURITY INCIDENT POLICY

1.0 POLICY STATEMENT

1.1 Denham Parish Council holds a large amount of information in a variety of formats stored in computers /books, printed documents and images in the forms of photographs. This includes personal and sensitive personal data and also nonpersonal 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.

2.0 SCOPE OF THE POLICY

2.1 This policy defines an Information Security Incident and sets out the Parish Council's procedures to follow on the reporting of an information security incident
(also referred to as a 'data breach').
2.2 This document 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 Denham 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.

3.0 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 accidently or on purpose.

4.0 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
- Transfer of data or information to those who are not entitled to receive that information
- Failure of equipment or power leading to loss of data
- Environmental – deterioration pf paper records
- 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 a third-party access)

5.0 WHEN TO REPORT THE BREACH

5.1 All information security breaches should be reported immediately to the Council via the Clerk.
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 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 them to investigate and confirm that the details represent a valid security incident as defined above.
5.5 The Parish Council is responsible for maintaining a confidential log of all information security events.

6.0 INVESTIGATION AND RESPONSE

6.1 Denham Parish Council will consider the report, and be responsible for investigation 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 practical.
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, what the legal and commercial consequences of the breach may be.
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 individual and the Parish Council.
6.5 Denham Parish Council will be responsible for formally recording the incident and the associated response. This report will be submitted to the Parish Council.

7.0 ESCALATION & NOTIFICATION

7.1 The Parish Council will be responsible for the initial assessment
of an incidents severity based on scope, scale and risk of the incident.
7.2 If a personal data breach has occurred of such a scale 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.

7.3 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 and will be carried out by Denham Parish Council. Liaison with the Police and other authorities may be required for serious events.

8.0 REVIEW

8.1 Once the incident had been contained, the Council will
undertake a thorough review of the vent to establish the cause of the incident, the effectiveness of the response and will identify the area 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 who will put plans in place to resolve and avoid any future incidents occurring.