BURSTALL PARISH COUNCIL

INFORMATION SECURITY INCIDENT POLICY

1. Policy Statement

Burstall Parish Council (the Council) holds a large amount of information in a variety of formats stored in computers, files, printed documents and images in the form of photographs. This includes personal and sensitive data, and non-personal information which may be sensitive or commercially confidential.

The 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 unauthorized access.

2. Scope of the Policy

This Policy defines an Information Security Incident and sets out the Council's procedures to follow on the reporting of an incident (also referred to as a 'data breach').

This Policy applies to all councillors, committees, staff, contractual third parties and agents of the Council who have access to Information Systems or information used for Council purposes.

3. Definition

An Information Security Incident is an event which occurs when data or information held by the Council, in any format, is compromised by being lost, destroyed, altered, copied, stolen, transmitted, unlawfully accessed or used by unauthorized 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
- unauthorized 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 of paper records
- changes to information or data or system hardware or software characteristics without the Council's knowledge, instruction or consent
- unauthorized use of a system for the processing or storage of data
- data maliciously obtained by way of social engineering (i.e. a cyber-attack in which a user is 'tricked' into allowing third-party access).

5. When to Report the Breach

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

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

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 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.

The Chair of the Council will also be informed to enable them to investigate and confirm the that the details represent a valid security incident as defined above.
The Council is responsible for maintaining a confidential log of all information security breaches.

6. Investigation and Response
The Council will consider the report and investigate the circumstances and the effect(s) of the information security incident.

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

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.

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 Council.

7. Escalation and Notification
An initial assessment of an incident's severity will be based on scope, scale and risk of the incident.

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

If the breach is deemed to be of a sufficient seriousness (in line with ICO guidance) and concerns personal data, notice of the breach will be given to the 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 Council to mitigate the risks. Liaison with the Police and other authorities may be necessary for serious events.

8. Review
Once the incident has been contained, the Council will undertake a thorough review to establish the cause of the incident, the effectiveness of the response and will identify the area(s) that require improvement.

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

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