Parish Office, Sports Pavilion, Hundred Acre Way, Red Lodge, Suffolk, IP28 8FQ

Information Security Incident

Policy

Contents

Document Control		3
Document Amendment History		3
1	Purpose	4
2	Scope	4
3	Definition	4
4	An Information Security Incident includes:	4
5	When to report	4
6	Action on becoming aware of the incident	4
7	How to report	4
8	What to Report	5
9	Examples of Information Security / Misuse Incident Protocols	5
9.2	Malicious Incident	5
9.3	Access Violation	5
9.4	Environmental	6
9.6	Theft / loss Incident	6
9.7	Accidental Incident	6
9.8	Miskeying	6
10	Escalation	6

Document Control

Organisation	
Title	
Creator	
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 This document defines an Information Security Incident and the procedure to report an incident

2 Scope

2.1 This document applies to all Councillors, Committees, Departments Partners, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Red Lodge Parish Council purposes.

3 Definition

3.1 An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is not entitled to receive it, or data is at risk from corruption.

4 An Information Security Incident includes:

- The loss or theft of data or information
- The transfer of data or information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent
- Unwanted disruption or denial of service to a system
- The unauthorised use of a system for the processing or storage of data by any person.

5 When to report

5.1 All events that result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported as soon as they happen.

6 Action on becoming aware of the incident

6.1 Follow the information security procedure, according to the type of incident.

7 How to report

7.1 The Community Action Suffolk IT Department must be contacted by email or telephone. They will log the incident and forward it on to the relevant departments.

7.2 The Community Action Suffolk IT Department will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident

- The type of data or information involved
- Whether the loss of the data puts any person or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of data or equipment affected
- Type and circumstances of the incident.

7.3 Your line manager must also be informed to enable them to investigate and confirm that the details represent a valid security incident as defined above. The outcomes of these actions are to be reported to the Community Action Suffolk IT Department for inclusion in the incident details for the Information Security Manager.

8 What to Report

8.1 All Information Security Incidents must be reported.

9 Examples of Information Security / Misuse Incident Protocols

9.1 Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

9.2 Malicious Incident

- Computer infected by a Virus or other malware, (for example spyware or adware)
- An unauthorised person changing data
- Receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Social engineering - Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).
- Unauthorised disclosure of information electronically, in paper form or verbally.
- Falsification of records, Inappropriate destruction of records
- Denial of Service, for example
- Damage or interruption to Red Lodge Parish Council equipment or services caused deliberately e.g. computer vandalism
- Connecting non-council equipment to the council network
- Unauthorised Information access or use
- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Printing or copying confidential information and not storing it correctly or confidentially.

9.3 Access Violation

- Disclosure of logins to unauthorised people
- Disclosure of passwords to unauthorised people e.g. writing down your password and leaving it on display
- Accessing systems using someone else's authorisation e.g. someone else's user id and password
- Inappropriately sharing security devices such as access tokens

- Other compromise of user identity e.g. access to network or specific system by unauthorised person
- Allowing Unauthorised Physical access to secure premises e.g. server room, scanning facility, dept area.

9.4 Environmental

- Loss of integrity of the data within systems and transferred between systems
- Damage caused by natural disasters e.g. fire, burst pipes, lighting etc
- Deterioration of paper records
- Deterioration of backup tapes
- Introduction of unauthorised or untested software
- Information leakage due to software errors.

9.5 Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Personal use of services and equipment in work time
- Using unlicensed Software
- Misuse of facilities, e.g. phoning premium line numbers.

9.6 Theft / loss Incident

- Theft / loss of data – written or electronically held
- Theft / loss of any Red Lodge Parish Council equipment including computers, monitors, mobile phones, Blackberries, Memory sticks, CDs.

9.7 Accidental Incident

- Sending an email containing sensitive information to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature, e.g. containing pornographic, obscene, racist, sexist, grossly offensive or violent material
- Receiving unsolicited mail which requires you to enter personal data.

9.8 Miskeying

- Receiving unauthorised information
- Sending information to wrong recipient.

10 Escalation

10.1 Serious incidents will be escalated via the national WARP scheme if determined to be of national value.