NORTON ON DERWENT TOWN COUNCIL

INFORMATION SECURITY INCIDENT POLICY

Purpose

This document defines an Information Security Incident and the procedures to report such incident.

Scope

This document applies to all councillors, employees, and contractual third parties and agents of the council who have access to information systems or information used.

Definition

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 of corruption.

Inclusions

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 (failed or successful) to gain unauthorised access to data or information on a computer system.

Changes to information or data or system hardware, firmware or software characteristics without the councils 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.

When to Report

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

How to Report

The Clerk must be contacted in person, by email or telephone and they will log the incident. You will be asked to supply some or all of the following information.

Contact name and number of the person reporting the incident.

Type of data / information involved.

Whether the loss puts any person or other data at risk.

Location of the incident.

Log details of the equipment affected.

Date and time of the incident.

The clerk will take appropriate mitigation action, providing a solution or calling our 3rd party systems manager, who will in turn, provide a solution. The matter will be reported to the council at inception, and a final report to the council once the matter has been resolved.

Serious Incidents

The police may be informed should the clerk and 3rd party systems manager deem it appropriate to do so, again the council will be kept informed of this.

Examples of Incidents / Misuse

Computer infected by a Virus or other malware.

An unauthorised person changing data or unauthorised information access.

Receiving and forwarding chain letters.

Unauthorised disclosure of information electronically, in paper form or verbally.

Falsification of records.

Inappropriate destruction of records.

Computer vandalism.

Connecting non council equipment to the council network.

Disclosure of logins to unauthorised people.

Deterioration of backup tapes and paper records.

Damage by natural disaster.

Accessing inappropriate material on the internet.

Sending inappropriate emails.

Using unlicensed software.

Sending an email containing sensitive information to ‘all staff’ by mistake.

Norton On Derwent Town Council, May 2018, Minute Number 013