YEOVIL TOWN COUNCIL

INFORMATION SECURITY INCIDENT POLICY

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, volunteers, employees, contractual third parties and agents of the Council who have access to Information Systems or information used for Yeovil Town 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.

3.2 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; and
- The unauthorised use of a system for the processing or storage of data by any person.

4. When to report

4.1 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.

5. Action on becoming aware of the incident

5.1 The Town Clerk must be informed immediately.

5.2 The Town Clerk will log the incident and may require further information depending on the nature of the incident. However, the following must be provided as a minimum:

- Contact name and number of person reporting the incident;
- The type of data or information involved;
- Whether the loss of the data put any personal or other data at risk;
- Location of the incident;
- Details of any equipment affected;
- Data and time the security incident occurred; and
- Circumstances of the incident.

6. Examples of Information Security / Misuse Incident Protocols

6.1 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 e-mails 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;
- Damage or interruption to equipment or services caused deliberately e.g. computer vandalism;
- Connecting non-council equipment to the local area network (not including Wi-Fi);
- Unauthorised information access or use;
- Giving information to someone who should not have access to it – verbally, in writing or electronically; and
- Printing or copying confidential information and not storing it correctly or confidentially.

6.2 Malicious Incident

- Disclosure of logins to unauthorised people;
- Disclosure of passwords to unauthorised people (e.g. wiring down passwords 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 use identity (e.g. access to network or specific system by unauthorised person); and
- Allowing unauthorised physical access to secure premises.

6.3 Environmental

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

6.4 Inappropriate use

- Accessing inappropriate material on the internet; and
- Using unlicensed software.

6.5 Theft/loss incident

- Theft/loss of data – written or electronically held; and
- Theft/loss of any Yeovil Town Council equipment including computers, mobile phones, laptops, memory sticks and CDs.

6.6 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); and
- Receiving unsolicited mail which requires you to enter personal data.

6.7 Mis-keying

- Receiving unauthorised information; and

- Sending information to unauthorised recipients outside of the Council domain.

6.8 Escalation

- Serious incidents will be escalated via the National WARP (Warning, Advice and Reporting Point) Scheme if determined to be of national value.

Yeovil Town Council
29th May 2018
To be reviewed: May 2019