INFORMATION INCIDENT POLICY 2019

Purpose

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

Scope

This document applies to all councillors and employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Woodbridge Town Council purposes.

Definition

An information security incident occurs when data or information is transferred or is at risk of being transferred to somebody who is entitled to receive it, or data is at risk of corruption.

An information Security Incident includes:

- The loss or theft of data 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.

When to Report

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.

Action on Becoming Aware of the Incident

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

How to Report

The Town Clerk must be contacted by e-mail or telephone. They will log the incident and forward it to the relevant recipients.

The Town Clerk 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 the 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.

The Town Clerk will 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 Council.

Information Security/Misuse Incident Protocols

All information Security Incidents must be reported. Information Security Incidents are not limited to the following lists which contain examples of some of the most common incidents:

- 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 on to others;
  - Social engineering – unknown people asking for information which could gain them access to council data (for example a password or details of a third party);
  - Unauthorised disclosure of information electronically, in paper form or verbally;
  - Falsification or records or inappropriate destruction of records;
  - Denial of service
  - Damage or interruption to Council equipment or services caused deliberately, for example computer vandalism;

    - Connecting non-Council equipment to the Council network;
    - Unauthorised information access or use;
    - Giving information to someone who should not have it either verbally, in writing or electronically;
    - Printing or copying confidential information and not storing it correctly or confidentially.
- Access violation:
    - Disclosure of logins to unauthorised people;
    - Disclosure of passwords to unauthorised people, including writing down your password and leaving it one display;
    - Accessing systems using someone else's authorisation, for example some else's user name and password;
    - Inappropriately sharing security devices;
    - Other compromise of user identity, for example access to network or specific system by unauthorised person; allowing unauthorised physical access to secure premises.
- Environmental:
    - Loss of integrity of the data within systems and transferred between systems;
    - Damage caused by natural disaster, for example fire, burst pipes, lighting;
    - Deterioration of paper records;
    - Introduction of unauthorised or untested software;
    - Information leakage due to software errors.
- Inappropriate use:
    - Accessing inappropriate material on the internet;
    - Sending inappropriate e-mails;
    - Sending an e-mail of an offensive nature, for example containing pornographic, obscene, racist, sexist, bullying, harassing, grossly offensive or violent material;
    - Personal use of services and equipment in work time;
    - Using unlicensed software;
    - Misuse of facilities, for example telephoning premium line numbers.
- Theft/loss incident:
    - Theft/loss of data, written or electronically held;
    - Theft/loss of any Council equipment including computers, monitors, mobile phones, memory sticks, CDs or other equipment that may be introduced.
- Accidental incident:
    - Sending an e-mail containing sensitive information to 'all staff' or 'all councillors by mistake;
    - Sending an e-mail to a Councillor's private e-mail address;
    - Receiving unsolicited mail of an offensive nature, for example containing pornographic, obscene, racist, sexist, bullying, harassing, grossly offensive or violent material;
    - Receiving unsolicited mail which requires you to enter personal data.

- Miskeying
    - Receiving unauthorised information;
    - Sending information to wrong recipient.