MAULDEN PARISH COUNCIL
Information Security Incident Policy

Adopted: May 2018
Next Review Date: Annually

1 PURPOSE
This document defines an Information Security Incident within Maulden Parish Council (MPC) and the procedure to report such an incident.

2 SCOPE
This document applies to all MPC Councillors, employees, contractual third parties and agents of MPC who have access to information systems or information used for MPC purposes.

3 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 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 MPC'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
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
Follow the information security procedure, according to the type of incident.

7 HOW TO REPORT
7.1 MPC's Clerk must be contacted by email or telephone who will log the incident.
7.2 MPC's Clerk will require the incident reporter 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 MPC's Clerk will investigate and confirm if the details represent a valid security incident as defined above.

8 WHAT TO REPORT
All Information Security Incidents must be reported to MPC's Clerk and then to the Information Commissioner's Office (ICO) as deemed necessary.
MPC's ICO reference number is **ZA353315**, and the ICO contact details are:
Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF
Email: mail@ico.gsi.gov.uk
Telephone: 0303 123 1113

9 EXAMPLES OF INFORMATION SECURITY / MISUSE INCIDENT PROTOCOLS
Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

9.1 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 emails which encourage the recipient to forward onto others.

- Social engineering – unknown people asking for information which could gain them access to MPC data (eg 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:
    a) Damage or interruption to MPC equipment or services caused deliberately, eg computer vandalism.
    b) Connecting non-MPC equipment to the MPC network.
    c) Unauthorised information access or use.
    d) Giving information to someone who should not have access to it – verbally, in writing or electronically,
    e) Printing or copying confidential information and not storing it correctly or confidentially.

9.2 Access Violation

- Disclosure of logins to unauthorised people.
- Disclosure of passwords to unauthorised people, eg writing down your password and leaving it on display.
- Accessing systems using someone else's authorisation, eg 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, eg server room, scanning facility, dept area.

9.3 Environmental

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

9.4 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, eg phoning premium line numbers.

9.5 Theft/loss Incident

- Theft/loss of data – written or electronically held.
- Theft/loss of any MPC equipment including computers, monitors, mobile phones, Blackberries, memory sticks, CDs.

9.6 Accidental Incident

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

9.7 Miskeying

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