# Information Security Incident Management Policy and Procedure.

Information Security Incident Management Policy and Procedure

- **Policy Statement**

  Aldington and Bonnington Parish Council will ensure that it reacts appropriately to any actual or suspected incidents relating to information systems and information within the custody of the Parish Council.

- **Purpose**

  This document states the Information Security Policy and Procedure for Aldington and Bonnington Parish Council. The policy establishes the principles and working practices that are to be followed by all users in order to ensure that any actual or suspected security incidents relating to information systems and data are dealt with promptly and effectively.

- **Scope**

  This policy applies to all Aldington and Bonnington Parish Council employees, councillors, contracted third parties and agents of the Parish Council with access to Aldington and Bonnington Parish Council's IT facilities, equipment and data. All users have responsibility for the safe and secure use of technology and data to which they have access.

  All users must understand and adopt use of this policy and are responsible for ensuring the safety and security of the Parish Council's systems and the information that they use or manipulate.

  All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

- **Definition**

  This policy must be followed as soon as information systems or data are suspected to be, or are actually affected by an adverse event which is likely to lead to a security incident.

  The definition of an "information management security incident" (information Security Incident" in the remainder of this policy and procedure) is a single or series of unwanted or unexpected events that threaten privacy or information security leading to damage to an organisation's assets, reputation and / or personnel, incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

  An Information Security Incident includes, but is not restricted to, the following:

  - 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 Parish 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.

Examples of some of the more common forms of Information Security Incidents have been provided in Appendix A.

- **Risks**

  Aldington and Bonnington Parish Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

  This policy aims to mitigate the following risks:

  - To reduce the impact of information security breaches by ensuring incidents are followed up correctly.
  - To help identify areas for improvement to decrease the risk and impact of future incidents.

  Non-compliance with this policy could have a significant effect on the efficient operation of the Parish Council and may result in financial loss and an inability to provide essential services to our customers.

- **Procedure for incident handling.**

  It is imperative that actual or suspected security incidents are contained as quickly as possible to minimise and manage the potential impact and damage of a security incident on the Parish Council. Users must report all events, threats and weaknesses to the Parish Clerk as soon as possible so that any or actual security incidents can be assessed, contained and resolved or prevented.

  The Parish Clerk will inform the Chairman and Vice-Chairman of the Parish Council of any incidents that have occurred, are occurring or likely to occur.

- **Policy compliance.**

  Any user found to have breached this policy may be subject to Aldington and Bonnington Parish Council's disciplinary procedures. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

  If any employee, councillor, contracted third party or agent of the Parish Council does not understand the implications of this policy or how it applies to them should seek advice.

- **Review and revision.**

  This policy, and all related appendices, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

**Appendix A**

**Examples of Information Security Incidents**.

Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

Malicious:

- Giving information to someone who should not have access to it – verbally, in writing or electronically.
- Computer infected by a Virus or other malware.
- Sending a sensitive email to 'all' by mistake.
- Sending an email with "PROTECT", "RESTRICTED" or higher classification content to a lower classified domain by mistake.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited email which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Unknown people asking for information which could gain them access to council data (e.g. a password or details of a third party).

Misuse:

- Use of unapproved or unlicensed software on Aldington and Bonnington Parish Council equipment.
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password)
- Writing down your password and leaving it on display / somewhere easy to find.
- Sending an email with "PROTECT", "RESTRICTED" or higher classification to a lower classified domain deliberately.
- Printing or copying confidential information and not storing it correctly or confidentially.

Theft / loss

- Theft / loss of a hard copy file.
- Theft / loss of removable data storage device or media, e.g. USB sticks, CDs external disk drives.
- Theft / loss of any Aldington and Bonnington Parish Council computer equipment.