

# **ALDERWASLEY PARISH 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 and Employees of Alderwasley Parish Council (The Council), contractual third parties and agents of the Council who have access to Information Systems or information used for the Council's 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.

## **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 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.

## **5 When to report**

- 5.1 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.

## **6 How to report**

- 6.1 The Clerk must be contacted by email with the following information:

- 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 What to Report**

7.1 All Information Security Incidents must be reported.

## **8 Examples of Information Security / Misuse Incident Protocols**

8.1 Information Security Incidents are not limited to this list, which contains examples of some of the most common incidents.

### **8.2 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 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
- Denial of Service, for example
- Damage or interruption to the Council's equipment or services caused deliberately e.g. computer vandalism
- Connecting non-Council equipment to the Council network
- Unauthorised Information access or use
- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Printing or copying confidential information and not storing it correctly or confidentially.

### **8.3 Access Violation**

- Disclosure of logins to unauthorised people
- Disclosure of passwords to unauthorised people e.g. writing down your password 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 user identity e.g. access to network or specific system by unauthorised person
- Allowing Unauthorised Physical access to secure premises e.g. server room, scanning facility, dept area.

### **8.4 Environmental**

- Loss of integrity of the data within systems and transferred between systems
- Damage caused by natural disasters e.g. fire, burst pipes, lighting etc
- Deterioration of paper records
- Deterioration of backup tapes
- Introduction of unauthorised or untested software

- Information leakage due to software errors.

#### 8.5 **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, e.g. phoning premium line numbers.

#### 8.6 **Theft / loss Incident**

- Theft / loss of data – written or electronically held
- Theft / loss of any of the Council's equipment including computers, monitors, mobile phones, Blackberries, Memory sticks, CDs.

#### 8.7 **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
- Receiving unsolicited mail which requires you to enter personal data.

#### 8.8 **Miskeying**

- Receiving unauthorised information
- Sending information to wrong recipient.

### 9 **Escalation**

#### 9.1 The Clerk will evaluate the information and must

- No later than 72 hours after having become aware of it, notify the personal data breach to the Council's Data Protection Officer and the ICO unless the personal data breach is *"unlikely to result in a risk for the rights and freedoms of individuals"*
- Where a personal data breach is likely to result in a **high risk** to the rights and freedoms of individuals, communicate the nature of the personal data breach together, in clear and plain language, to the data subject concerned, without undue delay unless:
  - The Clerk has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach (such as encryption).
  - The Clerk has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise.
  - It would involve disproportionate effort.

#### 9.2 Consider changes to policies and procedures in order to prevent future breaches