Great Barford Parish Council

Information Security Incident Policy

Purpose

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

Scope

This document applies to all Councillors, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Great Barford Parish Council (the 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 not entitled to receive it, or data is at risk from corruption.

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.

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 Clerk must be contacted by email or telephone. They will log the incident and forward it on to the relevant departments.

The 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 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
- Details of any equipment affected
- Date and time the security incident occurred
- Location of data or equipment affected
- Type and circumstances of the incident.

The outcomes of these actions are to be reported to the Clerk for inclusion in the incident form (Appendix A).

What to Report

All Information Security Incidents must be reported (Appendix A).

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.

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 Council equipment or services caused deliberately e.g. computer vandalism

- Connecting non-council equipment to the Council IT equipment
- 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.

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
- Other compromise of user identity e.g. access to network or specific system by unauthorised person

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
- Introduction of unauthorised or untested software
- Information leakage due to software errors.

Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Using unlicensed Software
- Misuse of facilities, e.g. phoning 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.

Accidental Incident

- Sending an email containing sensitive information to 'all' 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.

Miskeying

- Receiving unauthorised information
- Sending information to wrong recipient

Notifying breaches to the ICO

Under GDPR when a personal data breach has occurred, the Council needs to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then the Council must notify the ICO; if it is unlikely then the Council does not have to report it. However, if the decision is taken that the Council does not need to report the breach, it needs to be able to justify the decision, so it should be documented.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

The Council is required to report a personal data breach, which meets the reporting criteria, within 72 hours to the Information Commissioner and in some cases data subjects will have to be notified too. More details can be provided after 72 hours, but before then the ICO will need to know the potential scope and the cause of the breach, mitigation actions the Council plans to take and how the Council plans to address the problem.

In line with the accountability requirements, all data breaches must be recorded along with details of actions taken.

Appendix A - Data Breach Reporting Form

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	
Details of Breach	
Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states?	

What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	