Melksham Town Council

Data Security Incident Policy

Date Adopted: 24th November 2025

Date Due For Review: November 2027

DATA SECURITY INCIDENT POLICY

1. Introduction

We have a responsibility to ensure that personal information is kept and used securely. If anything goes wrong and, for example, data is lost, stolen, misused, sent to the wrong address or inappropriately accessed or released, we equally have a responsibility to put things right.

All suspected information security incidents must be reported to the Data Protection Officer (DPO). This enables the DPO to conduct a full investigation, and to identify areas of weakness and improvements that need to be made. It also enables the DPO to take a decision as to whether the incident should be reported to the Information Commissioner's Office as a data breach. The latter must be done within 72 hours of discovery. Therefore, all suspected incidents must be reported to the DPO as soon as they are discovered.

When sensitive information has been put at risk, but has not actually been lost, stolen, misused or inappropriately accessed or released, it may not be an incident requiring reporting to the Information Commissioner's Office however it is not good practice. For example, a member of staff taking sensitive information home without authority but returning it safely the next day would have put data at risk. The DPO will still put measures in place to prevent a reoccurrence.

All staff and councillors must be made aware of this procedure.

2. Procedure

All identified incidents must be reported to the DPO as soon as they are detected. Even where there is some difference of opinion regarding breach, err on the side of caution and report it.

Upon detecting a breach, it is important to act quickly. In particular it is important to let the DPO know the following:

- The extent of the breach
- The amount of information involved
- The sensitivity of information involved

The DPO will investigate the incident and establish why it happened, whether or not it constitutes a breach and what remedial action is necessary.

The DPO will use their initial assessment to report the breach if it meets the necessary threshold for reporting to the Information Commissioner's Office within 72 hours of the discovery of the breach. If this is done after 72 hours, the DPO will provide an explanation for this.

The DPO will prepare an incident report containing the following:

- A timeline of dates and times concerning the incident
- The potential for loss or damage to individuals, the Town Council or any other body
- What measures need to be taken and how quickly to address:-

    i. Restoring any lost information to our custody or control
    ii. Whether to warn people about the loss, including who to warn and when. This may require a risk assessment.
    iii. Factors taken into account for deciding to report the loss to the Information Commissioner's Office.
    iv. Whether to report the loss to the Police.

The DPO will consider taking statements from those involved, especially where the quality of evidence may be lost through time or people may not be present for long.

The DPO will report any actions that need to be taken to prevent a re-occurence of the breach and the Town Council will ensure that these are implemented.

The DPO will write to any data subject(s) affected, if necessary, dependent on the outcome of a risk assessment, and deal with any subsequent complaint. A standard letter template for this is in Appendix 1.

The DPO will also correspond as applicable with any member of the public reporting a breach.

The DPO will deal with any correspondence from the Information Commissioner's Office, providing any further information requested and implementing any recommendations.

APPENDIX 1

Letter to notify that personal data has been breached

Subject: Important Security Notice Regarding Your Personal Data

Dear **[Recipient Name]**,

We are writing to inform you of a data security incident that may have involved some of your personal information. We sincerely regret this incident and take the security of your data very seriously.

What happened?
On **[Date]**, we became aware of a data breach that occurred at Melksham Town Council**.** The incident happened because **[clearly describe what happened, e.g., an employee accidentally sent a file to the wrong recipient, a cyber-attack, a lost device]**.

What information was involved?
The data involved may include **[list the categories of personal data, e.g., your name, address, date of birth, email address, phone number, etc.]**. To the best of our knowledge, the following information was **not** involved: **[if possible, state what was not compromised, e.g., bank account details, national insurance numbers, etc.]**.

What are the potential consequences?
Based on the data involved, there may be risks such as **[describe the likely consequences, e.g., phishing attempts, identity theft, financial fraud, damage to reputation. Be specific based on the data compromised]**.

What we are doing
Upon discovering the breach, we took immediate action, including:

- **[Describe the immediate actions taken, e.g., Securing the affected systems, launching an investigation, notifying the Information Commissioner's Office (ICO)]**.
- **[Describe any further measures to mitigate harm, e.g., We are working to limit the effects, we have implemented additional security measures to prevent future incidents]**.

What you can do
To help protect yourself, we recommend that you:

- **[Provide specific guidance for the individual, e.g., Be vigilant against phishing scams, monitor your bank accounts, change passwords for any affected accounts]**.
- **[Include any additional information relevant to the type of breach, e.g., If bank details were involved, please alert your bank]**.

For more information
We understand you may have questions or concerns. If so, please d**o not hesitate to get in touch with me**. We will update you if there are any significant developments.

You may also wish to look at information available on the website of the Information Commissioner's Office, which can be accessed via this link https://ico.org.uk/for-the-public/ .

We deeply regret any harm or concern this incident may have caused you.

Sincerely,

[Name]
[Title]