DATA SECURITY INCIDENT PROCEDURE

GP5

DOCUMENT INFORMATION	
Item	**Details**
Policy Number	GP5
Policy Title	Data Security Incident Procedure
Responsible Committee	Policy Committee
Lead Officer	Town Clerk
Administered By	Deputy Town Clerk
Policy Version	3.0
Date of Previous Review	April 2023
Date Approved	November 2026 TBC
Review Frequency	Every 2 Years
Next Review Due	October 2028

1. Introduction

1.1 Bicester Town Council has a responsibility to ensure that personal data is collected, stored, used and shared securely and in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Where personal data is lost, stolen, altered, disclosed without authority, sent to the wrong recipient or otherwise compromised, the Council will take prompt action to contain the incident, assess the risk and implement appropriate corrective measures.

1.2 All suspected or actual information security incidents must be reported immediately to the Data Protection Officer (DPO). This enables the DPO to conduct a full investigation, assess the impact of the incident, identify weaknesses in procedures or controls, and determine any corrective actions required.

It also enables the DPO to take a decision as to whether the incident constitutes a personal data breach under the UK GDPR and Data Protection Act 2018, and whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required.

The latter must be done within 72 hours of the Council becoming aware of the breach; therefore, all suspected or actual incidents must be reported to the DPO as soon as they are discovered.

1.3 When personal data 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 should still be reported to the Data Protection Officer (DPO) and it is not good practice. For example, a member of staff taking personal data 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 recurrence. Such incidents and near misses should be recorded and reviewed to identify lessons learned and improve controls.

1.4 All staff and councillors must be made aware of this procedure and receive appropriate data protection and information security awareness training.

2. Procedure

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

2.2 Upon detecting a suspected or actual information security incident, it is important to act quickly. In particular it is important to let the DPO know the following:

- The nature and extent of the incident
- The amount of information involved
- The sensitivity of information involved
- Any immediate action taken to contain the incident.

2.3 The DPO will investigate the incident and establish why it happened, whether or not it constitutes a personal data breach, assess any risks posed to affected individuals, and what remedial action is necessary.

2.4 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 (ICO) within 72 hours of the Council becoming aware of the breach. If this is done after 72 hours, the DPO will provide an explanation for this.

2.5 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 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 notify affected individuals of the incident, including who should be informed and when. This may require a risk assessment.
  iii. Factors taken into account for deciding to report the breach to the Information Commissioner's Office.
  iv. Whether to report the incident to the Police.

2.6 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.

2.7 The DPO will report any actions that need to be taken to prevent a recurrence of the breach, and the Council will ensure that these are implemented.

2.8 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.

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

DRAFT

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

DRAFT

Letter to notify that personal data has been breached.

I write to you to bring to your attention a personal data breach that unfortunately involves your personal data.

As you would imagine, we have taken this matter very seriously and are investigating the incident / have concluded our investigation into the incident.

The circumstances of the incident are as follows:
<give brief description of what has happened, for example, a letter intended for you was sent to another individual because of an administrative error. The other individual immediately notified the Council upon receipt and returned the letter.>

I am unable for reasons of confidentiality to go into details of my investigation, however, I am able to tell you that:
<state what remedial action(s) have been carried out and what measures have been implemented to prevent a recurrence, without breaching confidentiality>

If you have any questions or concerns regarding this letter, please get in touch with the Council using the contact details provided below.

I would again like to apologise for the incident and any concern or inconvenience it may have caused.

Yours sincerely,
Town Clerk
Bicester Town Council

DRAFT

Letter in response to a reported data security incident.

Thank you for your letter / telephone call of <date> bringing the incident whereby <state what has happened> to our attention. We appreciate your assistance in helping the Council investigate and address this matter.

As you would imagine, we have taken this matter very seriously and have concluded our investigation into the incident.

The circumstances of the incident are as follows:
<give brief description of what has happened, for example, a letter intended for another individual was sent to you because of an administrative error>.

I am unable for reasons of confidentiality to go into details of my investigation; however, I am able to tell you that:
<state what remedial action(s) have been carried out and what measures have been implemented to prevent a recurrence, without breaching confidentiality>

I hope this letter has allayed your fears as to the integrity of your own information and documents, and I again thank you for bringing this matter to our attention and enabling the Council to take appropriate action.

Yours sincerely,
Town Clerk
Bicester Town Council

DRAFT