Okehampton Town Council

DRAFT Data Security Breach Response Policy and Procedure

Introduction

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorised use, equipment failure, human error, unforeseen circumstances such as a fire or flood, hacking attack, 'blagging' offences where information is obtained by deceiving the organisation who holds it.

A breach can happen in many ways, the following list describes some of the most common, but is not exhaustive:

- Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals.
- A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc.
- Sending or coping an email to an unintended recipient
- Accessing of records for no proper legitimate purpose
- Improper deletion or alteration of records

More information can be found using the link: https://ico.org.uk/for-organisations/gdpr-resources/pdb/

Who does this procedure apply to?

If you work for the Council, whether as an employee, contractor or in any other way, then this procedure applies to you. Councillors are also required to conduct themselves in accordance with this procedure.

What to do if a data breach is known or suspected

If you have reason to believe that a data breach has or may have happened you must complete a Data Breach Report Form as fully as possible and as soon as possible. The completed form must be sent to the Town Clerk, or in their absence the Assistant Clerk.

Responding to a Data Breach Report

On receipt of a Data Breach Report Form the Town Clerk, or Assistant Town Clerk, will invoke and follow the procedure as set out in Appendix 1, the responsibility for which may be delegated to the Assistant Town Clerk by the Town Clerk.

The incident will then be reported to the next meeting of Full Council or Policy and Resources Committee, whichever sooner.

APPENDIX 1

Okehampton Town Council
Data Breach Report Form

Details of Breach (Describe briefly what has happened or how the data breach arose with dates and times where possible)	
Nature and content of data involved (Describe the type(s) of personal information involved, eg email addresses, payroll information etc)	
Number of individuals affected	
Name of person making this report	
How and to whom this report was submitted	
Date and time this report was submitted	

Date and time of Notification of Breach	
Notification of Breach received from	

How and when report acknowledged	
Details of person investigating	
Any further information about the breach	
Information Commissioner informed, if relevant Time and method of report and by whom https://report.ico.org.uk/security-breach/	
Police informed if relevant Time and method of report and by whom	

Individuals contacted How many individuals contacted? Method of contact used? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that the 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: what technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response, to include notification of the Full Council	