Minehead Town Council

Data Breach Policy and Data Security Breach Reporting Form

Adopted

Data Breach Policy

GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

• Access by an unauthorised third party.

• Deliberate or accidental action (or inaction) by a controller or processor.

• Sending personal data to an incorrect recipient.

• Computing devices containing personal data being lost or stolen.

• Alteration of personal data without permission.

• Loss of availability of personal data.

Minehead Town Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a Personal Data Breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Minehead Town Council duty to report a breach:

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

The Finance and General Purposes Committee must be informed immediately so that it is able to report the breach to the ICO in the 72-hour timeframe.

If the ICO is not informed within 72 hours, Minehead Town Council via the Finance and General Purposes Committee must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Minehead Town Council must:

1. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

2. Communicate the name and contact details of the Finance and Governance Committee.

3. Describe the likely consequences of the breach.

4. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

When notifying the individual affected by the breach, Minehead Town Council must provide the individual with (2)-(4) above.

Minehead Town Council will not need to communicate with an individual if the following applies:

• It has implemented appropriate technical and organisational measures (i.e., Encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it.

• It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or, • It would involve a disproportionate effort.

However, the ICO must still be informed even if the above measures are in place.

Records of Data Breaches

All data breaches must be recorded whether they are reported to individuals. This record will help to identify system failures and should be used to improve the security of personal data.

Date of Breach	Type of Breach	Number of Individuals affected	Date reported to ICO/Individual	Actions to prevent breach recurring

To report a data breach, Minehead Town Council will use the ICO online system:

https://ico.org.uk/for-organisations/report-a-breach

Data Security Breach Reporting Form

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.

Use this form to report such breaches.

Example:

• Reportable 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.

More information can be found using the below link:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-andresources/security/a-guide-to-data-security/

Breach Containment and Recovery

Article 2(2) of the Notification Regulation states:

The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system.

PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security reaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date & time of notification of breach.	
Notification of breach to whom: Name Contact Details	
Details of breach	

Nature & 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 & method of contact https://ico.org.uk/for-organisations/report-a - breach/	
Police informed if relevant. Time & method of contact Name of person contacted. Contact details.	

Individuals contacted. How many individuals contacted. Method of contact. What are the potential consequences & adverse effects on those individuals? Confirm the details of the nature of the risk to the individuals affected? Provide any measures that they can take to minimise any affects.	
Staff Briefed.	
Assessment of ongoing risk.	
Containment actions: technical & organisational security measures you have applied or about to apply to the affected personal data.	
Recovery Plan	
Evaluation & response	