BREACH NOTIFICATION POLICY

FAVERSHAM
TOWN COUNCIL

Contents

Adopted Date	2018
Review Period	2 years
Last Review Date	December 2025
Next Review Date	June 2027

BREACH NOTIFICATION POLICY

1. Scope

This procedure applies in event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

The GDPR draws a distinction between a data controller and a data processor in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller or a data processor for the same data processing activity; it must be one or the other.

2. Responsibility

All users (whether employees/staff, contractors or temporary employees/staff and third party users) and Councillors of Faversham Town Council are required to be aware of, and to follow this procedure in the event of a personal data breach.

3. Identify a Personal Data Breach/Suspected Personal Data Breach

A personal data breach can happen for a number of reasons, for example:

- Loss or theft of data or equipment on which data is stored, or through which it can be accessed
- Loss or theft of paper files
- Hacking attack
- Inappropriate access controls allowing unauthorised/unnecessary access to data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood

4. Reporting an Incident

Any individual who accesses, uses or manages the Council's information is responsible for reporting data breach and information security incidents immediately to the Town Clerk.

If the breach occurs outside of normal working hours, it must be reported as soon as is practicable.

The report must contain full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the

nature of the information, and how many individuals are involved. A Data Breach Report Form should be completed as part of the reporting process.

5. Record of Data Breaches

Date of Breach	Type of Breach	Number of Individuals Affected	Date Reported to ICO/Individual	Actions to Prevent Breach Recurring

6. Investigation

Depending on the type and severity of the incident the Town Clerk will assess whether a full investigation into the breach is required. Where required the Town Clerk will appoint a Lead Investigation Officer who will complete a full breach report.

The investigation will:

a) Establish the nature of the incident, the type and volume of data involved and the identity of the data subjects
b) Consider the extent of a breach and the sensitivity of the data involved
c) Perform a risk assessment
d) Identify actions the organisation needs to take to contain the breach and recover information
e) Assess the ongoing risk and actions required prevent a recurrence of the incident.

7. Reporting Breach to the Information Commissioner or Data Subject

The Town Clerk will co-ordinate breach reporting to the Information Commissioner within 72 hours of becoming aware of a relevant breach. They will also evaluate whether the breach is '*likely to result in a high risk to the rights and freedoms'* of the data subject. If this is determined to be the case the incident it will also be reportable to the data subjects without undue delay. Any such report will be coordinated by the Town Clerk, assistance may be required from Officers and Councillors.

8. Evaluation

Once the initial incident has been contained, the Town Clerk will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.