West Mersea
Town Council

DATA BREACH POLICY

1. DATA BREACH POLICY

1.1. The General Data Protection Regulations 2018 define 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.

West Mersea Town Council takes the security of personal data seriously. Computers are password protected and hard copy files are kept in locked cabinets.

2. CONSEQUENCES OF A PERSONAL DATA BREACH

2.1. 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.

3. DUTY TO REPORT A BREACH

3.1. Data breaches do not have to be routinely notified to the Information Commissioner's Office (ICO) or others. GDPR makes informing the ICO and the individuals affected compulsory in certain circumstances.

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

3.3. If appointed, the Data Protection Officer (DPO), otherwise the Proper Officer, must be informed immediately. The DPO or Proper Officer must report the breach to the ICO. If the ICO is not informed within 72 hours, the DPO or Proper Officer must give reasons for the delay when they report the breach.

4. WHEN NOTIFYING THE ICO OF A BREACH, THE COUNCIL MUST:

- Describe the nature of the breach including the cause and scope (type of data, approximate number of data subjects and data records concerned);
- Communicate the name and contact details of the DPO, or Proper Officer;
- Describe the likely consequences of the breach;
- Describe the measures taken or proposed to be taken to address the personal data breach including mitigation measures and future preventative actions.

5. WHEN NOTIFYING AN INDIVIDUAL OF A BREACH, THE COUNCIL MUST:

- Communicate the name and contact details of the DPO, or Proper Officer;
- Describe the likely consequences of the breach;
- Describe the measures taken or proposed to be taken to address the personal data breach including mitigation measures and future preventative actions.

The Council will not need to notify an individual if the following applies:

- It has previously implemented appropriate technical and organisational measures such that the personal data is unintelligible to any person not authorised to access it (e.g. encryption);
- 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.

6. DATA PROCESSOR'S DUTY TO INFORM WEST MERSEA TOWN COUNCIL

6.1. If a data processor (e.g. payroll provider) becomes aware of a personal data breach, it must notify the Council without undue delay, so that the Council can fulfil its responsibilities under this policy.

7. RECORDS OF DATA BREACHES

7.1. All data breaches must be recorded. This record should be used to identify system failures and to improve the security of personal data.

- Date of breach
- Type of breach
- No. individuals affected
- No. records affected
- Reporting date to ICO/individual
- Cause of breach
- Likely consequences Preventative actions taken

Data breaches should be reported to the ICO via:
https://ico.org.uk/for-organisations/report-a-breach/

Adopted: 7 November 2019, Minute ref: 19/240
Review Date: 25 November 2021, Minute ref: 21/277
Review: November 2022