Littlehampton Town Council

Personal Data Breach Policy

This personal data breach policy sets out the procedures we have put in place to deal with a breach of the confidentiality integrity or availability of personal data within our organisation.

We are Littlehampton Town Council a council in England. Our contact details are The Manor House, Church Street, Littlehampton, West Sussex, BN17 5EW, 01903 732063, ltc@littlehampton-tc.gov.uk

We are a data controller for personal data as defined by all applicable data protection and privacy laws including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the “UK GDPR”), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation (the “Data Protection Legislation”).

This policy is binding on all employees, councillors and volunteers (“User" or "Users”) of Littlehampton Town Council (“The Organisation”) in order to protect Personal or other Data ("Personal Data" or "Data”) processed by the organisation.

It applies to all organised filing systems be they computer based, paper based or any other such method of organising information which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (“Filing Systems”).

1. Definitions

1.1. “Personal data” means any information relating to an identified or identifiable individual (“data subject”); an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

1.2. Personal data will typically contain information about the individual or their activities.

1.3. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. This includes breaches that are the result of both accidental and deliberate causes.

1.4. Personal Data breaches can include but are not limited to:

1.4.1. Access by an unauthorised third party.

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

1.4.3. Sending personal data to an incorrect recipient.

1.4.4. Computing devices containing personal data being lost or stolen.

1.4.5. Paper files containing personal data being lost or stolen.

1.4.6. Alteration of personal data without permission, and

1.4.7. Loss of availability of personal data.

1.5. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

1.6. There will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed or if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

2. Who is responsible for managing personal data breaches

2.1. The Town Clerk is responsible for the ongoing compliance monitoring of this and other policies that are designed to achieve compliance with the Data Protection Legislation. In the absence of the Town Clerk, users must contact the next most senior officer available (“the person responsible for data protection”).

2.2. No user within the organisation shall deviate from this policy without written authorisation from the person responsible for data protection.

3. Time limits

3.1. Not all personal data breaches are reportable to the Information Commissioner's Office (“ICO”) but those that are must be reported within 72 hours of ‘becoming aware’ of a breach.

3.2. The 72 hour time frame is irrespective of bank holidays or weekends.

3.3. Users who suspect there has been a breach must notify in writing the person responsible for data protection within 1 hour of becoming aware of the suspected breach.

4. Investigation

4.1. The person responsible for data protection shall undertake an investigation of a suspected personal data breach to ascertain the circumstances of the breach and whether or not the breach was a result of human error or a systemic issue.

4.2. The investigation should consider if a recurrence can be prevented.

4.3. If human error is the cause of the personal data breach, the investigation should consider if:

4.3.1. Data protection induction and refresher training for users is adequate.

4.3.2. Support and supervising of users in their role is adequate.

4.3.3. Policies and procedures require updating.

4.4. If the breach was caused by a systemic issue, the investigation should consider if:

4.4.1. Access levels are fit for purpose.

4.4.2. If a wider system audit should be undertaken.

4.4.3. Do technical and organisational measures to maintain data security need to be reviewed.

4.4.4. Do additional technical and organisational measures to maintain data security need to be implemented?

4.5. Council must be informed of any breach, “lessons learned” from investigations and ICO feedback where given.

5. Notifying the ICO

5.1. The ICO must be notified of breaches where there is a **likelihood** of risk to people's rights and freedoms.

5.1.1. If a risk is likely, the person responsible for data protection must notify the ICO within 72 hours of 'becoming aware' of a breach.

5.1.2. If a risk is unlikely, there is no requirement to report it, but a voluntary report may still be made if the person responsible for data protection so decides.

5.2. If a breach has occurred and it has been decided not to report to the ICO then the decision and reasons shall be documented by the person responsible for data protection in the Littlehampton Town Council breach register.

5.3. If a breach has occurred and it has been reported to the ICO then the decision and reasons shall be documented by the person responsible for data protection in the Littlehampton Town Council breach register.

6. Telling data subjects

6.1. If there has been a personal data breach where there is a **likelihood** of risk to people's rights and freedoms the person responsible for data protection should contact those individuals affected and:

6.1.1. Describe, in clear and plain language, the nature of the personal data breach and, at least:

6.1.1.1. The name and contact details of the person responsible for data protection as a point where more information can be obtained.

6.1.1.2. A description of the likely consequences of the personal data breach, and

6.1.1.3. A description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects.

6.2. If possible, the person responsible for data protection should give specific and clear advice to individuals on the steps they can take to protect themselves, and what Littlehampton Town Council are willing to do to help them.

6.2.1. Advice could include but is not limited to:

6.2.1.1. A password reset.

6.2.1.2. Advising individuals to use strong, unique passwords.

6.2.1.3. Telling individuals to look out for phishing emails or fraudulent activity on their accounts.

7. Users role in personal data breach

7.1. Users must notify in writing the person responsible for data protection immediately and in any case within 1 hour of any actual or suspected personal data breach.

7.2. No user should try to rectify a breach without first informing and getting authorisation from the person responsible for data protection.

7.3. Users must provide all timely assistance to the person responsible for data protection in the course of their investigation.

7.4. Obstruction of the investigation will be addressed via the relevant disciplinary procedure.

8. Updates to this policy

8.1. This policy shall be reviewed every four years by the person responsible for data protection.

8.2. This policy shall be reviewed if Littlehampton Town Council makes changes to the organisations Privacy Notice or if there are changes to how the organisation processes data or the data protection legislation changes.

8.3. This policy was last updated on 17.10.2024.

9. Implementation

9.1. This policy takes effect from 17.10.2024 and is not retroactive.