Personal Data Erasure Policy

Date **please insert date of adoption** (which must match the resolution number)

Edition No and Date: 1 / XX.XX.2024

Replaces Data Protection Policy 30.03.2017 *to be discarded*

Policy Maker Jon Short, Deputy Town Clerk

Responsibility Policy and Finance

Resolution Number **please insert resolution number from minutes (DD.MM.YY. / Min.Min.Min.)**

Review Cycle Every 3 years or earlier in the event of legislative change

This information pack contains:

Personal Data Erasure Policy
Policy 1: Personal Data Erasure Policy

For reviews with no changes or minor changes only – agreed by Town Clerk and Deputy Town Clerk.
N/A

Draft

Littlehampton Town Council

Personal Data Erasure Policy

This personal data erasure policy sets out the procedures we have put in place to deal with the erasure 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. **Definition of personal data**

   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.

2. **Who is responsible for managing erasure of personal data**

   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. ("the person responsible for data protection").

Draft

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

3. Erasure

3.1. Personal data should be erased when:

3.1.1. The personal data is no longer necessary for the purpose which it was originally collected or processed for. Normal retention periods are specified in the Privacy Notice and Retention Schedule.

3.1.2. The organisation is relying on consent as the lawful basis for processing the data, and the individual withdraws their consent.

3.1.3. The organisation is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.

3.1.4. The organisation is processing the personal data for direct marketing purposes and the individual objects to that processing.

3.1.5. The organisation has processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle).

3.1.6. The organisation has to do it to comply with a legal obligation, or

3.1.7. The organisation has processed the personal data to offer information society services to a child.

3.2. The right to erasure does not apply if processing is necessary for one of the following reasons:

3.2.1. To exercise the right of freedom of expression and information.

3.2.2. To comply with a legal obligation.

3.2.3. For the performance of a task carried out in the public interest or in the exercise of official authority.

3.2.4. For archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing, or

3.2.5. For the establishment, exercise or defence of legal claims.

Draft

3.3. The UK GDPR also specifies two circumstances where the right to erasure does not apply to special category data:

3.3.1. If the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices), or

3.3.2. If the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

3.4. The organisation may refuse to comply with a request if it is:

3.4.1. Manifestly unfounded. A request may be manifestly unfounded if:

3.4.1.1. The individual clearly has no intention to exercise their right of erasure. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation, or

3.4.1.2. The request is malicious in intent and is being used to harass the organisation with no real purposes other than to cause disruption.

3.4.2. Excessive. A request may be excessive if:

3.4.2.1. It repeats the substance of previous requests; or

3.4.2.2. It overlaps with other requests.

3.4.3. The person responsible for data protection shall decide if a request is manifestly unfounded or excessive on a case-by-case basis. The organisation does not have a blanket policy on refusal.

3.4.4. All requests should be considered in the context in which it is made.

Draft

3.4.5. If a request is refused the person responsible for data protection should document why they consider the request is manifestly unfounded or excessive.

3.5. In the event of the right to erasure not being applicable or the organisation refusing the request to erase, the person responsible for data protection will inform the individual without undue delay and within 28 days of receipt of the request and provide:

3.5.1. The reasons the organisation is not taking action.

3.5.2. The individual's right to make a complaint to the ICO, and

3.5.3. The individual's ability to seek to enforce this right through a judicial remedy.

4. Time limits

4.1. The person responsible for data protection must respond to an erasure request without undue delay and at the latest within 28 calendar days with confirmation of erasure or reasons for refusal.

4.2. The time limit to respond starts on receipt of the request or (if later) on receipt of any information requested to confirm the requestor's identity.

4.3. The person responsible for data protection can extend the time to respond by a further two months if the request is complex or they have received a number of requests from the individual. The person responsible for data protection must let the individual know within 28 calendar days of receiving their request and explain why the extension is necessary.

4.4. If the person responsible for data protection has doubts about the identity of the person making the request, they can ask for more information to identify them. They should only request information that is necessary to confirm identity. The person responsible for data protection must inform the individual without undue delay and within 28 calendar days that they need more information to confirm identity.

5. Users role in erasure requests

5.1. The organisation has a legal responsibility to identify that an individual has made a request.

5.2. The UK GDPR does not specify how to make a valid request. A request can be made verbally or in writing. It can also be made to any

part of the organisation and does not have to be to a specific person or contact point.

5.3. Users should be aware that requests can be made via email, or social media.

5.4. A request does not have to include the phrase 'request for erasure' or Article 17 of the UK GDPR.

5.5. Users must notify in writing the person responsible for data protection immediately and in any case within 1 working day of a request to erase.

5.6. No user should action the erasure request and erase data without first informing and getting authorisation from the person responsible for data protection.

5.7. Users must provide all timely assistance to the person responsible for data protection.

5.8. Obstruction of a lawful erasure by a user will be addressed via the relevant disciplinary procedure.

6. Erasure of data

6.1. When data is to be erased either because it is no longer required to fulfil the purpose for which it was collected or because there has been a valid request to erase from the data subject in question, the person responsible for data protection shall ensure that:

6.1.1. Paper based personal data is cross cut shredded or disposed of via a secure disposal contractor who supplies a certificate of destruction, and / or

6.1.2. Electronic records are removed from backup systems as well as live systems.

6.1.2.1. The organisation is aware that when data is deleted from the live system it will remain within the backup environment for a certain period of time until it is overwritten.

6.1.2.2. For erasure where the data is no longer required this time delay is acceptable and backups can be allowed to run to normal schedule as the data will be erased from them in due course.

Draft

6.1.2.3. For data that has been requested to be erased the person responsible for data protection must confirm to the requester what will happen to their data when their erasure request is fulfilled, including in respect of backup systems, an indication should be given of how long it will take to purge from the backups. The person responsible for data protection should then ensure that the data on the backup is 'beyond use' and that the data within the backup is not used for any other purpose.

6.2. The person responsible for data protection must ensure that data that has been erased is not accidentally reintroduced in the event of a backup being restored.

6.3. When actioning erasure the person responsible for data protection shall ensure that the relevant data is erased from the entire filing system paying particular attention to file location whether centralised, decentralised or dispersed on a functional or geographical basis.

7. Updates to this policy

7.1. This policy shall be reviewed every three years by the person responsible for data protection.

7.2. 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.

7.3. This policy was last updated on [date].

8. Implementation

8.1. This policy takes effect from [date] and is not retroactive.

Draft