Subject Access Request Policy

Date XX.XX.2024 (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:

Subject Access Request Policy
Policy 1: Subject Access Request Policy

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

Littlehampton Town Council

Subject Access Request Policy

This subject access request policy sets out the procedures we have put in place to facilitate responding to subject access requests 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 subject access requests**

   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").

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

3. Subject access request

3.1. Individuals have the right to access and receive a copy of their personal data, and other supplementary information.

3.2. Subject Access Request ("SAR") is a legal mechanism that has a very strictly defined and specific ambit.

3.3. It is a right that entitles a data subject to be informed by the organisation as to whether and how the organisation processes their personal data, a copy of that data and other supplementary information.

3.4. The parameters of the right are set out clearly in the UK GDPR which provides that a data subject "shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data".

3.5. Subject access request is not a right to request 'documents' and is different to the freedom of information laws.

3.6. The organisation believes that the right of access is key to allowing individuals to have real control over their own personal data, however there are times when the right of access can be refused wholly or partially.

3.7. A subject access request can be refused if it is:

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

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

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

3.7.3. Excessive. A request may be excessive if:

3.7.3.1. It repeats the substance of previous requests; or

3.7.3.2. It overlaps with other requests.

3.8. 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.

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

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

3.11. In the event of refusal of a subject access request the person responsible for data protection will inform the individual without undue delay and within 28 days of receipt of the request and provide:

3.11.1. The reasons the organisation is not taking action;

3.11.2. Their right to make a complaint to the ICO and,

3.11.3. Their ability to seek to enforce this right through a judicial remedy.

3.12. There are other exemptions that the person responsible for data protection must consider when preparing to disclose personal data to a SAR requestor.

3.13. If the response to the request would disclose personal data of another individual the person responsible for data protection shall make sure that the information has been redacted with a suitable redaction tool or method to maintain the confidentiality of the third party individual(s).

3.14. Schedules 2 and 3 of the UK Data Protection Act 2018 provide various other exemptions from subject access requests, the person responsible for data protection shall take professional advice on correct application of these exemptions if they are to be relied upon.

3.14.1. Crime and taxation: general.

3.14.2. Crime and taxation: risk assessment.

3.14.3. Legal professional privilege.

3.14.4. Functions designed to protect the public.

3.14.5. Regulatory functions relating to legal services, the health service and children's services.

3.14.6. Other regulatory functions.

3.14.7. Judicial appointments, independence and proceedings.

3.14.8. Journalism, academia, art and literature.

3.14.9. Research and statistics.

3.14.10. Archiving in the public interest.

3.14.11. Health, education and social work data.

3.14.12. Child abuse data.

3.14.13. Management information.

3.14.14. Negotiations with the requester.

3.14.15. Confidential references.

3.14.16. Exam scripts and exam marks.

3.14.17. Other Exemptions.

4. Time limits

4.1. The person responsible for data protection must respond to a subject access request without undue delay and at the latest within 28 calendar days with a copy of the personal data and other supplementary information or reasons for whole or partial 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 subject access 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 phrases 'subject access request', ‘right of access’ or ‘Article 15 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 subject access request or suspected subject access request.

5.6. No user should action the subject access request and gather personal data without first informing and getting authorisation from the person responsible for data protection.

5.7. If the person responsible for data protection asks, the user should follow this template from the ICO to gather details from the requestor Subject access request template for small businesses | ICO

~~5.6.~~5.8. Users must provide all timely assistance to the person responsible for data protection in their gathering and preparation of personal data for a subject access request.

~~5.7.~~5.9. Obstruction of the collection of personal data for a subject access request by a user will be addressed via the relevant disciplinary procedure.

6. Supply of personal data to the requestor

6.1. The right of access also entitles an individual to other supplementary information.

6.1.1. The organisations purposes for processing;

6.1.2. Categories of personal data the organisation is processing;

6.1.3. Recipients or categories of recipient the organisation has or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);

6.1.4. The organisations retention period for storing the personal data or, where this is not possible, the criteria for determining how long the organisation will store it;

6.1.5. The individual's right to request rectification, erasure or restriction or to object to processing;

6.1.6. The individual's right to lodge a complaint with the Information Commissioner's Office (ICO);

6.1.7. Information about the source of the data, if the organisation did not obtain it directly from the individual;

6.1.8. Whether or not the organisation uses automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and

6.1.9. The safeguards the organisation has provided where personal data has or will be transferred to a third country or international organisation.

6.2. The person responsible for data protection should ensure that all of the above items of supplementary information are detailed in the organisation's privacy notice.

6.2.1. If they are not, the privacy notice should be updated without delay, or

6.2.2. If they are, the requirement to supply supplementary information can be complied with by supplying a copy of the organisations privacy notice.

6.3. If the individual submitted the SAR electronically (e.g. by email or via social media), The person responsible for data protection must provide the supplementary information and a copy of the personal data in a commonly used electronic format.

6.4. The person responsible for data protection may choose the format, unless the requester makes a reasonable request for it to be provided in another commonly used format (electronic or otherwise).

6.5. If the individual submitted the SAR by other means (e.g. by letter or verbally), the person responsible for data protection can provide a copy in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for it to be provided in another commonly used format.

6.6. The person responsible for data protection should ensure that the transfer of the personal data to the requester is done via an appropriately secure method.

6.7. The right of access enables individuals to obtain their personal data rather than giving them a right to see copies of documents containing their personal data.

6.8. The person responsible for data protection may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out or copy of the relevant information from the organisation's filing system.

6.9. When supplying in a commonly used format the requester must not be required to take any specific action in order to access the data. For example, being required to buy or download software.

6.10. If the requester asks for the information in hard copy, Royal Mail special delivery is considered a secure method of sending the information.

6.11. The person responsible for data protection may need to explain some of the information provided when responding to a SAR if the individual may have difficulty understanding it.

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.