Data Protection Policy

CONTENTS

Adopted: October 2018
Review Date: August 2023

1. INTRODUCTION

Totton & Eling Town Council (the Council) supports the objectives of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) and seeks to ensure compliance with this data protection legislation.

The processing of data by the Council is essential to services and functions, at times involving the use of personal data, and compliance with the data protection legislation will ensure that such processing is carried out fairly and lawfully.

The Council is open and transparent about its operations and works closely with the community. In the case of information that is not personal or confidential, the Council is prepared to make information available to the public as per the Council's Publication Scheme.

2. SCOPE

This Data Protection Policy applies to all Council employees, Councillors, volunteers and contractors. See the 'Roles & Responsibilities' section of this policy for more information.

This policy governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information.

This policy provides a framework within which the Town Council will ensure compliance with the data protection legislation and will underpin any operational procedures and activities connected with the implementation of the legislation.

3. POLICY STATEMENT

The Town Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under data protection legislation. The Council will use all appropriate and necessary means at its disposal to comply with data protection legislation through this adopted Data Protection Policy.

4. DATA PROTECTION LEGISLATION

The GDPR and DPA govern the rights of individuals regarding their personal data and the way in which this data is controlled and processed by those with legitimate reasons for using the personal information. It provides a mechanism by which individuals about whom the data is held ('data subjects') can have a certain amount of control over the way in which it is handled.

4.1. Core Principles

The regulations are based on six core principles with a new principle of accountability meaning the Council must ensure compliance. This is achieved through the Council producing and maintaining documents that demonstrate what actions have been taken to achieve compliance, such as privacy notices and consent forms clearly showing for what purpose the data is being used and demonstrating that data subjects have 'opted in'.

4.1.1. ***Lawfulness, Fairness & Transparency*** – processed lawfully, fairly and in a transparent manner in relation to the data subject.

4.1.2. ***Purpose*** – Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.1.3. ***Data Minimisation*** – Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4.1.4. ***Accuracy*** – Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

4.1.5. ***Storage Limitation*** – Kept in a form which permits identification of data subjects for no longer than in necessary for the purposes for which the personal data are processed.

4.1.6. ***Integrity and Confidentiality*** – Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition to the above principles, the data protection legislation sets out specific strengthened sanctions over sharing data outside the European Economic Area. This requires councils to ensure appropriate privacy safeguards are in place when using cloud-based services. The Council's data is backed up by Schools ICT (computer networks) in the United Kingdom and Microsoft Office (email services) in three separate locations within the United Kingdom to ensure the safety of data.

4.2. Lawfulness of Processing

The data protection legislation sets out six lawful bases for processing personal data.

Unless an exemption applies, at least one of these will apply in all cases where personal data is processed by the Council; often a number of different lawful bases will apply at the same time. For example, the Council may be performing a task in the public interest, under a legal obligation e.g. processing data in the exercise of a statutory power, and sometimes as a result of contractual necessity.

In addition to the lawful bases below, the Council will ensure additional conditions are met, in accordance with the legislation, with regards to the processing of any sensitive personal information.

4.2.1. ***Consent***

i. A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language.

ii. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by a clear affirmative action.

4.2.2. ***Legitimate interests***

i. This involves a balancing test between the controller (or a third party's) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

ii. Please note, councils and parish meetings are public authorities and under the GDPR public authorities cannot rely on legitimate interests as a legal basis for processing personal data.

4.2.3. ***Contractual necessity***

i. Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

4.2.4. ***Compliance with legal obligation***

i. Personal data may be processed if the controller is legally required to perform such processing e.g. complying with the requirements of legislation.

4.2.5. ***Vital Interests***

i. Personal data may be processed to protect the 'vital interests' of the data subject e.g. in a life or death situation it is permissible to use a person's medical or emergency contact information without their consent.

4.2.6. ***Public Interest***

i. Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

4.3. Individual Rights

The Council will ensure that individuals on whom personal information is kept are aware of their rights under data protection legislation and have access to that information on request.

Subject to some legal exceptions, individuals will have the rights below:

4.3.1. ***Right to access personal data the Council holds on you*** – At any point you can contact the Council to request the personal data held on you, as well as why the Council has that personal data, who has access to the personal data and where the data was obtained from.

4.3.2. ***Right to correct and update the personal data the Council holds on you*** – If the data the Council holds on you is out of date, incomplete or incorrect, you can inform the Council and your data will be updated.

4.3.3. ***Right to have your personal data erased*** – If you feel that the Council should no longer be using your personal data or that the Council is unlawfully using your personal data, you can request that the Council erase the personal data it holds.

4.3.4. ***Right to object to processing of your personal data or to restrict it to certain purposes only*** – you have the right to request that the Council stop processing your personal data or ask the Council to restrict processing.

4.3.5. ***Right to data portability (personal data transferred from one data controller to another)*** – You have the right to request that the Council transfer some of your data to another controller.

4.3.6. ***Right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*** – You can withdraw your consent easily by telephone, email or by post.

4.3.7. ***Right to lodge a complaint with the Information Commissioner's Office*** – You can contact the Information Commissioner's Office via contact details on their website at https://ico.org.uk/global/contact-us/

The process for making a request for personal data the Council holds on you (a 'Subject Access Request') or any similar requests as above is set out as an addendum to this policy.

5. ROLES & RESPONSIBLITIES

5.1. Data Protection Officer

Within DPA 2018 it was agreed that Town and Parish Councils are not required to appoint an external Data Protection Officer as is required by other 'public authorities'.

The Council does however have an internally appointed Data Protection Officer, the Executive Support Officer, who is responsible for the following tasks:

5.1.1. Informing and advising the Council, any processor engaged by the Council as data controller, and any employee of the Council who carries our processing of personal data, of that person's obligations under the legislation.

5.1.2. Providing advice and monitoring for the carrying out of data protection impact assessments.

5.1.3. Co-operating with the Information Commissioner's Office, acting as the contact point for the Information Commissioner's Office.

5.1.4. Assigning responsibilities under the Council's data protection policies, raising awareness of the policies, training staff involved in processing operations and conducting audits required under those policies.

The Council will provide the Data Protection Officer with the necessary resources and access to personal data and processing operations to enable them to perform the tasks outlined above and to maintain their expert knowledge of data protection law and practice.

5.2. Town Council

The Town Council will be responsible for ensuring that the organisations complies with its responsibilities under the data protection legislation through monitoring or activities and incidents via reporting by the Data Protection Officer.

5.3. All Staff & Councillors

All staff and councillors will ensure that:

5.3.1. Personal information is treated in a confidential manner in accordance with this and any associated policies.

5.3.2. The rights of data subjects are respected at all times.

5.3.3. Privacy notices will be made available to inform individuals how their data is being processed.

5.3.4. Personal information is only used for the stated purpose, unless explicit consent has been given by the data subject to use their information for a different purpose.

5.3.5. Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.

5.3.6. Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.

5.3.7. Personal information is recorded accurately and is kept up to date.

5.3.8. Records they are responsible for retaining are disposed of in accordance with the Council's Data Retention Policy, by shredding or other confidential method where required.

5.3.9. They refer any subject access requests and/or requests in relation to the rights of individuals to the Data Protection Officer.

5.3.10. They raise actual or potential breaches of the DPA to the Data Protection Officer as soon as the breach is discovered.

It is the responsibility of all staff and councillors to ensure that they comply with the requirements of this policy and any associated policies or procedures.

5.4. Contractors and Employment Agencies

Where contractors are used, the contracts between the Council and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same code of behaviour as Town Council members of staff and councillors in relation to data protection legislation.

5.5. Volunteers

All volunteers are bound by the same code of behaviour as Town Council members of staff and councillors in relation to data protection legislation. It is the staff member's responsibility that is arranging volunteer work to ensure that the volunteers are aware of the responsibilities on them under this policy.

6. DATA RETENTION

Good records management plays a vital role in ensuring that the Council is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meeting the requirements of the data protection legislation. Data must only be used for the purpose it was gathered for and should be deleted when it is no longer needed for that purpose.

All records will be retained and disposed of in accordance with the Council's Document Retention Policy. Sensitive or confidential documents are disposed of by shredding or other means to ensure that the material can no longer be read or interpreted.

No document list can be exhaustive. Questions regarding the retention period for any specific document or class of document not in the Council's Document Retention Policy should be addressed to the Data Protection Officer.

7. INFORMATION REQUESTS

7.1. Personal Data

Requests from data subjects for copies of personal data the Council holds about them ('Subject Access Requests') or any other requests for information under the individual rights of data protection legislation should ideally be made in writing but can also be made verbally.

The Subject Access Request procedure, covering submitting subject access requests and the Council responding, is provided as an addendum to this policy.

7.2. Non-Personal Data

The Council's Publication Scheme is a means by which the Council can make a significant amount of information routinely available without waiting for someone to specifically request it.

In accordance with the Freedom of Information Act 2000, this scheme specifies the classes of information which the Council published or intends to publish, as well as an information guide giving

greater detail of what the Council will make available. This aims to make it easier for public to access information.

Requests for information that is not personal data can be made verbally or in writing and will be dealt with in accordance with the Council's Freedom of Information Request Policy.

Much of the Councils information is however available on its website at www.tottoneling-tc.gov.uk and individuals are encouraged to first look on the website for the information they seek.

8. COMPLAINTS

Any expression of dissatisfaction from an individual with reference to the Council's handling of personal information will be treated as a complaint and handled under the Council's Complaints Procedure. The Data Protection Officer will be involved in responding to the complaint.

Should the complainant remain dissatisfied with the outcome of their complaint to the Council, a complaint can be made to the Information Commissioner's Office who will then investigate the complaint and take action where necessary.

The contact details for the Information Commissioner Office can be found online at https://ico.org.uk/global/contact-us/

Subject Access Request Procedure

1. What is a Subject Access Request?

A Subject Access Request (SAR) is a written request made by or on behalf of an individual for personal data held on said individual which he or she is entitled to ask for under data protection legislation.

2. How do I submit a SAR?

A SAR must be made either verbally or in writing and can be in any form; it does not have to include certain phrases such as 'subject access' or 'data protection legislation'.

It is recommended that a SAR be submitted in writing to the Council either via post or via email to info@tottoneling-tc.gov.uk, requests may however also be submitted via social media, the Council's website or any other written means of contact.

Due to the nature of SARs and the communication required, a request submitted via social media or the website will often need to be supplemented with another form of communication; ideally email.

It is recommended that, for the ease of identifying the exact request, the written request clearly set out:

a. The individual the request is regarding (the 'data subject')

b. The information/data you are requesting (the 'personal data')

c. How you would like to receive the data e.g. electronically via email, posted paper copies etc. The default format will be electronic, wherever possible.

3. What process will the Council follow to respond?

Upon receipt of a SAR, this will be passed to the Town Clerk (or in their absence, the Deputy Town Clerk) to undertake the following process:

<u>Upon Receipt of a SAR</u>

a. Verify that the Council is the controller of the data subject's personal data that is being requested. If the Council is not the controller, but merely a processor, you will be informed so and referred to the data controller.

b. Verify the identity of the data subject; if needed, the Council may request further evidence that you are the data subject (the Council will provide a list of example identification that will be accepted). If you are making the request on behalf of the data subject, the Council will need to satisfy itself that you are entitled to act on behalf of the individual. The Council does have the right to send the response direct to the data subject rather than through a third party, where it feels relevant.

c. Verify the access request; is it sufficiently substantiated? Is it clear what data you are requesting? If not, the Clerk will contact you for further information.

d. Verify whether requests are unfounded or excessive (in particular if in a repetitive character); if so, the Council may refuse to act on the request or charge a reasonable fee.

e. Promptly acknowledge receipt of the SAR and inform you of any costs involved in processing the SAR. Where a cost is to be incurred, the Clerk will await your agreement with the cost before proceeding with a response to your request.

f. Verify whether the Council processes any data requested by carrying out a full exhaustive search of all records. If no data is processed, the Clerk will inform you accordingly.

g. Verify whether the data requested also involves other data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, the Council will first have to ensure that other data subjects have consented to the supply of their data as part of the SAR.

Responding to a SAR

h. Respond to a SAR within one month after receipt of the request:

   (i) If more time is needed to respond to a complex request, an extension of another two months is permissible, provided this is communicated to you in a timely manner within the first month

   (ii) If the Council cannot provide the information requested it will inform you on this decision within one month of receipt of the request.

i. Where possible, the Council will include the following in its response:

   (i) The purpose for processing this data;

   (ii) The categories of personal data concerned;

   (iii) The recipients or categories of recipients to who the personal data has been or will be disclosed;

   (iv) Where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;

   (v) The existence of the right to request rectification or erasure of personal data or restriction of processing personal data concerning the data subject or to object to such processing;

   (vi) The right to lodge a complaint with the Information Commissioner's Office;

   (vii) If the data has not been collected from the data subject, the source of such data;

j. Provide a copy of all the personal data requested that the Council processes, unless an exemption applies.

k. The Council will ensure the data is in an 'intelligible form', which includes giving an explanation of any codes, acronyms and complex terms, where relevant.

l. The Council will not erase any data or change any data prior to a response to a SAR, unless this would have been done regardless of the SAR being received or not; under data protection legislation, the Council is not allowed to erase data to prevent it being released.

m. If the data cannot be supplied in a permanent form i.e. electronic or hard copies, the Council may request that you come and inspect any data on screen or files on its premises. This will need to be arranged at a mutually agreeable time.

n. The Council will maintain a record of all SARs received, the outcomes and showing compliance against the statutory timescales.

4. How will I receive the information?

Wherever possible, the Council will provide you with any personal data electronically, except where a request has been made otherwise or the data is not available electronically.

The Council may decline to supply information via social media if technological constraints make it impractical or if information security considerations make it inappropriate to do so. In these circumstances, the Council will ask you for an alternative delivery method for the response.

5. Will there be a cost?

SAR's will be undertaken free of charge to you unless the legislation permits reasonable fees be charged; this could be an administrative cost of complying with the request where the request is considered unfounded or excessive or where an individual requests further copies of their data following an original request.

6. Can the Council refuse to comply with a request?

If the Council believes the request is manifestly unfounded or excessive it can either request a 'reasonable fee' from you to deal with the request (an administration fee for locating and producing the data) or refuse to deal with the request. In either case, the Council will justify its decision.

If the request is refused or you are quoted a fee to produce the data, you will be informed of your right to make a complaint to the Information Commissioner's Office.

7. What data is exempt from a SAR?

Each SAR will be assessed on its own merits upon receipt and careful consideration given to whether or not an exemption applies. If any exemption applies the Council may refuse the release of that data or may be able to redact the data being disclosing it to the individual.

Any example of an exemption is where the personal data is 'legally privileged' because it is contained within legal advise provided to the Council or relevant to ongoing or preparation for litigation.

If an exemption is considered to apply, the Council will clearly set this out in its response to you.

The Council may seek external professional advice if it is felt necessary to determine whether an exemption applies and the best course of action.

8. What if I am unhappy with the response received?

If you are unhappy with the response received, you should inform the Council; this will then be dealt with as a complaint in accordance with the Council's Complaints Procedure.

If, once the complaint has been considered and decided upon by the Council, you are still unhappy with the outcome, you have a right to make a complaint to the Information Commissioner's Office.

The contact details for the Information Commissioner Office can be found online at https://ico.org.uk/global/contact-us/