Watton Town Council

Data Retention Policy

June 2024

---

1. INTRODUCTION

1.1 This Policy sets out the obligations of Watton Town Council ("the **Council**") regarding retention of personal data collected, held, and processed by the Council in accordance with the retained EU law version of Regulation 2016/679 General Data Protection Regulation ("UK GDPR"), as implemented by the Data Protection Act 2018. All references to UK GDPR include reference to the Data Protection Act 2018.

1.2 The UK GDPR defines "personal data" as any information relating to an identified or identifiable living individual (a "data subject"). An identifiable living 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.

1.3 The UK GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

1.4 Under the UK GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

1.5 In addition, the UK GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

1.5.1 Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

1.5.2 When the data subject withdraws their consent;

1.5.3 When the data subject objects to the processing of their personal data and the Council has no overriding legitimate interest;

1.5.4 When the personal data is processed unlawfully (i.e. in breach of the UK GDPR);

1.5.5 When the personal data is being used for direct marketing purposes, and the data subject objects to such processing;

1.5.6 When the personal data has to be erased to comply with a legal obligation; or

1.5.7 Where the personal data is processed for the provision of information society services to a child.

1.6 This Policy sets out the type(s) of personal data held by the Council, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

1.7 For further information on other aspects of data protection and compliance with the UK GDPR, please refer to the Council's Data Protection Policy.

2. AIMS AND OBJECTIVES

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Council complies fully with its obligations and the rights of data subjects under the UK GDPR.

2.2 In addition to safeguarding the rights of data subjects under the UK GDPR, by ensuring that excessive amounts of data are not retained by the Council, this Policy also aims to improve the speed and efficiency of managing data.

3. SCOPE

3.1 This Policy applies to all personal data held by the Council and by third-party data processors processing personal data on the Council's behalf.

3.2 Personal data, as held by the Council is stored in the following ways and in the following locations:

3.2.1 The Council's remote servers, which are further backed-up secured in other locations outside of these initial remote servers;

3.2.2 Computers permanently located in the Council's premises;

3.2.3 Laptop computers and other mobile devices provided by the Council to its officers, councillors and employees, but only in accordance with the limitations set in the Council's Data Protection Policy;

3.2.4 Physical records stored in the Council's premises and in secure offsite storage; and

3.2.5 Third party cloud storage providers and offsite records storage.

4. DATA SUBJECT RIGHTS AND DATA INTEGRITY

4.1 All personal data held by the Council is held in accordance with the requirements of the UK GDPR and data subjects' rights thereunder, as set out in the Council's Data Protection Policy.

4.2 Data subjects are kept fully informed of their rights, of what personal data the Council holds about them, how that personal data is used as set out in Part 5 of the Council's Privacy Policy, and how long the Council will hold that personal data (or,

if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.3 Data subjects are given control over their personal data held by the Council including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Council's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling, as set out in Part 11 of the Council's Privacy Policy.

5. TECHNICAL AND ORGANISATIONAL DATA SECURITY MEASURES

5.1 The following technical measures are in place within the Council to protect the security of personal data. Please refer to Parts 26 to 30 of the Council's Data Protection Policy for further details:

5.1.1 All emails containing personal data must be marked "confidential";

5.1.2 Personal data may only be transmitted over secure networks;

5.1.3 Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

5.1.4 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

5.1.5 Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using a signed for courier service;

5.1.6 All personal data transferred physically should be transferred in a suitable container marked "confidential";

5.1.7 No personal data may be transferred to any councillors, employees, workers, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without authorisation from the Data Compliance Manger, unless otherwise permitted in the course of your duties or under the provisions of the Council's Data Protection Policy;

5.1.8 No personal data should be transferred to any device personally belonging to any councillor, officer or employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Council where the party in question has agreed to comply fully with the Council's Data Protection Policy and the UK GDPR;

5.1.9 Personal data must not be transferred and/or transported using unencrypted removable media, such as USB drives, because they are insecure;

5.1.10 All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely, in either a locked box, drawer, cabinet or similar;

5.1.11 Personal data must be handled with care at all times and should not be left unattended or on view;

5.1.12 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Council or otherwise without the formal written approval of the Data Compliance Manager and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

5.1.13 Desks, filing cabinets and cupboards should be kept locked if they hold confidential information of any kind;

5.1.14 All personal data stored electronically should be backed up daily with backups stored onsite and offsite. All backups should be encrypted;

5.1.15 No personal data may be shared informally and if a councillor, or an employee, agent, sub-contractor, or other party working on behalf of the Council requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Compliance Manager (whose details are set out in the Data Protection Policy);

5.1.16 Computers used to view personal data must always be locked before being left unattended;

5.1.17 Only personnel who need to access the personal data will be permitted to have access;

5.1.18 Where personal data held by the Council is used for marketing purposes, it shall be the responsibility of the Town Clerk to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service. Evidence of the consent process and opt out will also be kept by the Town Clerk, and reviewed by the Data Compliance Manager;

5.1.19 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Council is designed to require such passwords;

5.1.20 Under no circumstances should any passwords be written down or shared between any councillors, officers, employees, agents, contractors or other parties working on behalf of the Council, irrespective of seniority. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

5.1.21 All software should be kept up-to-date. The Council's IT staff shall be responsible for installing any and all security-related updates not more than 14 days after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so;

5.1.22 No software may be installed on any Council-owned computer or device without approval of the IT Manager and the Data Compliance Manager.

5.2 The following organisational measures are in place within the Council to protect the security of personal data. Please refer to Part 31 of the Council's Data Protection Policy for further details:

5.2.1 All councillors, officers, employees, agents, contractors or other parties working on behalf of the Council shall be made fully aware of both their individual responsibilities and the Council's responsibilities under the UK GDPR and under the Council's Data Protection Policy;

5.2.2 Only councillors, officers, employees, agents, contractors or other parties working on behalf of the Council that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Council;

5.2.3 All councillors, officers, employees, agents, contractors and other parties working on behalf of the Council handling personal data:

(a) will be appropriately trained to do so;

(b) will be appropriately supervised;

(c) shall be required and encouraged to exercise care, caution and discretion when discussing any work relating to personal data at all times, and whether in the workplace or otherwise;

5.2.4 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

5.2.5 All personal data held by the Council shall be reviewed periodically, as set out in this Data Retention Policy;

5.2.6 The performance of those councillors, officers, employees, agents, contractors or other parties working on behalf of the Council handling personal data shall be regularly evaluated and reviewed;

5.2.7 All councillors, officers, employees, agents, contractors or other parties working on behalf of the Council handling personal data will be bound by contract to comply with the UK GDPR and the Council's Data Protection Policy;

5.2.8 All agents, contractors, or other parties working on behalf of the Council handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Council arising out of the UK GDPR and the Council's Data Protection Policy; and

5.2.9 Where any agent, contractor or other party working on behalf of the Council handling personal data fails in their obligations under the UK GDPR and/or the Council's Data Protection Policy, that party shall indemnify and hold harmless the Council against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. DATA DISPOSAL

6.1 Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1.1 Personal data stored electronically (including any and all backups thereof) shall be deleted securely using the relevant built in system tools after it has been reviewed by the Data Compliance Manager;

6.1.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely using the relevant built in system tools after it has been reviewed by the Data Compliance Manager;

6.1.3 Personal data stored in hardcopy form shall be shredded to at least European Standard EN15713 and recycled;

6.1.4 Special category personal data stored in hardcopy form shall be shredded to at least European Standard EN15713 and recycled.

7. DATA RETENTION

7.1 As stated above, and as required by law, the Council shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out in the Council's data retention register.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

7.3.1 The objectives and requirements of the Council;

7.3.2 The type of personal data in question;

7.3.3 The purpose(s) for which the data in question is collected, held, and processed;

7.3.4 The Council's legal basis for collecting, holding, and processing that data; and

7.3.5 The category or categories of data subject to whom the data relates.

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Council to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the UK GDPR.

8. ROLES AND RESPONSIBILITIES

8.1 The Council's Data Compliance Manager is Jane Scarrott - telephone number: 01953 881007, email address: clerk@wattontowncouncil.gov.uk, postal address: Watton Town Council, Wayland Hall, Middle Street, Watton, Norfolk IP25 6AG.

8.2 The Data Compliance Manager shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Council's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the UK GDPR and other applicable data protection legislation.

8.3 The Data Compliance Manager shall be directly responsible for ensuring compliance with the above data retention periods throughout the Council.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of UK GDPR compliance should be referred to the Data Compliance Manager.

9. IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of [●] 2024. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: [●]

Position: [●]

Date:

Due for Review by:

Signature: