Thaxted Parish Council

Data Retention Policy

1. Introduction

1.1 This Policy sets out the obligations of Thaxted Parish Council ("the Council") regarding retention of personal data collected, held, The General Data Protection Regulations (GDPR) which came into effect in May 2018 provided clear responsibilities for those collecting, using and protecting personal information in addition to those provisions as set out in the UK Data Protection Act 2018.

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

1.3 The 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 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. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

1.5 In addition, the 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:

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

b) When the data subject withdraws their consent;

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

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

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

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

1.2 This Policy sets out the type(s) of personal data held by the Council for the performance of an employment contact, compliance with a legal obligation & to protect the vital interests of the data

subject. 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.

1.3 For further information on other aspects of data protection and compliance with the 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 GDPR.

2.2 In addition to safeguarding the rights of data subjects under the 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 Councils behalf.

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

a) The Councils Computer, located in a locked room with restricted access, this is located at the Councils main office.

b) Laptop computers and other mobile devices provided by the Council to its employees.

c) Physical records stored in the main office in a locked file

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 GDPR and data subjects' rights thereunder, as set out in the Council's Data Protection Policy.

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 data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.2 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out in Parts 12 and 13 of the Company's Data Protection Policy, and how long the Company 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).

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 22 to 26 of the Council's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

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

e) 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;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient

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

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Dena Ludford Parish Clerk & RFO.

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Council or not, without authorisation;

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

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

n) No personal data should be stored on any mobile device, whether such device belongs to the Council or otherwise without the formal written approval of Dena Ludford Parish Clerk & RFO 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;

o) No personal data should be transferred to any device personally belonging to an 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 GDPR;

p) All personal data stored electronically should be backed up Daily with backups stored onsite AND offsite. All backups should be encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be changed regularly and should must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

t) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

u) No software may be installed on any Council-owned computer or device without approval; and

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

a) All employees and 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 GDPR and

under the Council's Data Protection Policy;

b) Only employees and 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;

c) All employees and other parties working on behalf of the Council handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Council handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Council handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

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

g) The performance of those employees and other parties working on behalf of the Council handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Council handling personal data will be bound by contract to comply with the GDPR and the Council's Data Protection Policy;

i) 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 GDPR and the Council's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Council handling personal data fails in their obligations under the 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:

(a) Personal data stored electronically (including any and all backups thereof) shall be deleted off the system. If these are being deleted from an email this does have a 90-day retention within the 'exchange' however after the 90 days this is deleted permanently, only the user of the email who deleted would be able to reinstate this.

(b) Personal data stored in hardcopy form shall be shredded & recycled.

(c) Special category personal data stored in hardcopy form shall be shredded 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 below.

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

(a) the objectives and requirements of the Council;

(b) The type of personal data in question;

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

(d) The Council's legal basis for collecting, holding, and processing that data;

(e) 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 GDPR.

Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
Surname	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	N/A
Forenames	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	N/A
Address, including postcode	Necessary for the performance of an employment contract	Every 12 Months	Duration of employment	N/A
Telephone number	Necessary for the performance of an employment contract	Every 12 Months	Duration of employment	N/A
Nationality	For compliance with a legal obligation (Right to work in the UK)	Every 12 Months	Duration of employment	Required as proof of right to work in the UK.
Date of Birth	Necessary for the performance of an employment contract – (Driving insurance, Minimum wage, Security Checks)	N/A	Duration of employment	N/A
Driving Licence details (Including points)	For compliance with a legal obligation & Necessary for the performance of an employment contract – (Driving insurance)	Every 6 Months	Duration of employment	Required for insurance purposes.
National Insurance Number	Necessary for the performance of an employment contract	N/a	Up to 6 Years after termination of employment	Maybe listed on pay records, pay records are required for up to 6 years in the event of a breach of contract claim.

Criminal Convictions	Necessary for the performance of an employment contract (DBS & Vetting)	Every 12 Months	Up to 6 Months after termination of employment	Required as employees working within a setting where vulnerable adults or children are present.
Emergency Contact details (Name and number)	Necessary to protect the vital interests of the data subject. (Required in case of an emergency)	Every 12 Months	Duration of employment	N/A
Conditions of employment	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of contract claim.
Holiday records	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of contract claim.
DBS Checks	Necessary for the performance of an employment contract & For compliance with a legal obligation.	Every 3 Years	Up to 6 Months after termination of employment (Only up to date copy kept on file)	Required as employees working within a setting where vulnerable adults or children are present
Vetting Checks	Necessary for the performance of an employment contact & For compliance with a legal obligation.	Every 18 Months	Up to 6 Months after termination of employment (Only up to date copy kept on file)	Required as employees working within a setting where vulnerable adults or children are present
Working time	For compliance with a legal	N/A	Up to 6 Years after termination of	Required for up to 6 years in the event of a breach of

opt out form	obligation.		employment	contract claim.
Training records (Including qualifications)	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Months after termination of employment	Maybe required in support of any potential unfair/constructive dismissal claim.
PPE Check list	Necessary for the performance of an employment contract, for compliance with a legal obligation & to protect the vital interests of the data subject.	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of health and safety claim.
Appraisal Records	Necessary for the performance of an employment contract.	Every 12 Months	Up to 6 Months after termination of employment (Only up to date copy on file)	Maybe required in support of any potential unfair/constructive dismissal claim.
Timesheet records.	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of contract claim.
P45 & P60	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of contract claim.
Disciplinary and/or capability records	For the purposes of the legitimate interest pursued by the data controller & Necessary for the performance of an employment contract	Every 12 Months	Only for duration of Live warning, unless dismissed kept for 6 Months after termination.	Maybe required in support of any potential unfair/constructive dismissal claim.

Pay records	Necessary for the performance of an employment contract	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of contract claim
Medical records / health questionnaires	Necessary to protect the vital interests of the data subject & for compliance with a legal obligation.	Every 12 Months	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of health and safety claim.
Sickness records	Necessary to protect the vital interests of the data subject & for compliance with a legal obligation.	Every 12 Months	Up to 6 Months after termination of employment	Maybe required in support of any potential unfair/constructive dismissal claim.
Training cost agreement	Necessary for the performance of an employment contract	Every 12 Months	Duration of Live agreement. Unless employee leaves before agreement has lapsed and then kept for up to 6 years after employment	Required for up to 6 years in the event of a breach of contract claim
Bank Account Details	Necessary for the performance of an employment contract	Every 12 Months	Duration of employment	N/A
P11D	For compliance with a legal obligation.	N/A	Up to 6 Years after termination of employment	Required for up to 6 years in the event of a breach of contract claim

8. Roles and Responsibilities

8.1 The Council's with a Data Protection Contact is Dena Ludford. And can be contact at Clerk@Thaxted.co.uk

8.2 The Data Protection Contact 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 GDPR and other applicable data protection legislation.

8.3 The Data Protection Contact 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 GDPR compliance should be referred to the Data Protection Contact.

9. Implementation of Policy

9.1 This Policy shall be deemed effective as of 00:00 hrs 26th April 2019. 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: Dena Ludford & Thaxted Parish Council

Position: Clerk & RFO

Date: 25th April 2019

Due for Review by: May 2021

Signature: