Thorney Parish Council

Information Protection Policy

May 2018

Adopted: 8 May 2018

Review: 9 May 2019

Document Control

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description

1 Purpose

1.1 Information is a major asset that **Thorney Parish Council has a duty and responsibility to protect.**

1.2 The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within or by the Council.

2 Scope

2.1 The Information Protection Policy applies to all Councillors, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Thorney Parish Council purposes.

2.2 The purposes for which personal data may be used by us:

Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes.

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring Council policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Improving services
- Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers, members of the public, Council service users, residents, correspondents

Personal data we gather may include: individuals' contact details, background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, physical or mental health or condition, criminal offences, or related proceedings in fact any use of sensitive personal data will be strictly controlled in accordance with this policy and **only asked for if relevant**

2.3 Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

2.4 Data portability

Upon request, a data subject will have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This will be done for free.

2.5 Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

2.6 Information takes many forms and includes:

- hard copy data printed or written on paper
- data stored electronically
- communications sent by post / courier or using electronic means
- stored tape or video
- speech

3 Information Storage

3.1 All electronic information will be stored on centralised facilities to allow regular backups to take place.

3.2 Information will not be held that breaches the Data Protection Act (1998), GDRP 2018 or formal notification and guidance issued by Thorney Parish Council.

3.3 Records management and retention policy will be followed.

3.4 Databases holding personal information will have a defined security and system management policy for the records and documentation.

3.5 This documentation will include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.

3.6 Files which are listed by Thorney Parish Council as a potential security risk should not be stored on the network, except for in designated application storage areas. To facilitate this Thorney Parish Council will implement an electronic File security solution.

4 Disclosure of Information - Computer and Paper Based

4.1 The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is be reported to the Data Control Officer (Clerk) who will take appropriate action.

4.2 Printed information will not be removed from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances

4.3 Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4.4 Disposal methods for waste computer printed output and other media must be shredded

4.5 Distribution of information should be via the most secure method available.

5 Disclosure of Information – Telephone, Fax and E-mail

Where this involves the exchange of sensitive information then the following procedures will be applied.

6 Telephone calls:

6.1 Verify identification before disclosing information. If in doubt, return their call using a known telephone number.

6.2 For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity

6.3 Ensure that you are authorised to disclose the information requested.

6.4 Ensure that the person is entitled to be given this information.

6.5 Ensure that the information you give is accurate and factual.

7 Fax transmissions:

Fax will not be used to transmit personal or sensitive information.

8 Disclosure of information by email:

8.1 Personal or sensitive information is at risk if sent outside of the Council's network.

8.2 If an e-mail is sent to an address that is not a Council domain address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted. Therefore

8.3 Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure (encryption)

8.4 The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

8.5 No identifiable personal information should be included when sending on emails.

8.6 The recipient of Thorney Parish Council emails are prohibited from being forwarded, copied or blind copied to any third party outside of the Council.

9 Sharing of Personal Information

9.1 Information relating to individuals shall not be shared with other authorities without the agreement of the Data Protection Officer.

9.2 Members should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

9.3 We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

9.4 **The Data Protection Officer's responsibilities:**

- Keeping the Council updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Assisting with data protection advice for all members and those included in this policy
- Answering questions on data protection
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by Thorney Parish Council.
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing

9.5 **Responsibilities of the Members**

- Approving data protection statements attached to emails
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all initiatives adhere to data protection laws and the company's Data Protection Policy