Thurcaston and Cropston Parish Council Data Protection Policy

The Data Protection Act 1998 Eight Principles of Good Practice.

1. Personal data shall be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with the purpose.
3. Personal data shall be adequate and relevant and not excessive in relation to the purpose for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up-to-date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance the rights of the data subject under this Act.
7. Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Six Conditions

At least one of the following conditions must be met for personal information to be considered fairly processed:

1. The individual has consented to the processing.
2. Processing is necessary for the performance of a contract with the individual.
3. Processing is required under a legal obligation (other than one imposed by the contract).
4. Processing is necessary to protect the vital interest of the individual.
5. Processing is necessary to carry out public functions e.g. administration of justice
6. Processing is necessary in order to pursue the legitimate interest of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual.

Sensitive Data

Specific provision is made under the Act for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.
For personal information to be considered fairly processed, at least one of several extra conditions must be met. These include:

- Having the explicit consent of the individual
- Being required by law to process the information for employment purposes
- Needing to process the information in order to protect the vital interests of the individual or another person

- Dealing with the administration of justice or legal proceedings

Guidance for Staff

The Data Protection Act 1998

The purpose of this statement is to provide guidance on the objectives of the Data Protection Act 1998 and the obligations under the Act which apply equally to Council Members and Staff.

1. Registration/notification

   The Clerk must be provided with sufficient information to enable them to give the Data Protection Commissioner notification of any registrable particulars of computer or a manual system where data is processed.

   Information regarding new systems or files or new uses of existing files shall be provided to the Clerk in sufficient time to enable notification details to be submitted before the new systems are brought into use or files created or used in any new way.

2. Unregistered personal data

   Unregistered or inaccurate personal data shall not be held. The Council's Clerk may examine both computers or manual data to determine the accuracy of registration and Staff and Members must co-operate in this process. If unregistered personal data is discovered it shall not be processed until registered.

3. Access Rights for Data Subjects

   Any requests received from an individual exercising the right of access to personal data MUST BE referred to the Clerk. The response to the application will be met as soon as possible and in any case within 40 days of a properly completed application.

4. Disclosure of Personal Data

   The categories of persons and organisations to whom disclosure outside these categories be made. If personal data includes data relating to another person care must be taken not to disclose that data without authorisation.

   (a) The Data Subject

   Care and reasonable steps must be taken to ensure proper identification when answering personal or telephone enquiries. In the case of written enquiries check that the name and address is the same as that of the data subject.

   (b) Family, Relatives, Guardians, Trustees, Legal and Financial Representatives, Banks, Building Societies, Insurance Companies and Voluntary / Charitable Organisations etc and Agents of the Data Subject

   (c) New Employer of the Data Subject

If a data subject's employer requests details, these should only be those relating to P45's and other statutory requirements. If anything beyond these requirements are sought, written authorisation or consent of the data subject himself must be obtained by the person requiring the information before information is disclosed to them by Thurcaston & Cropston Parish Council.

(d) Other Statutory Bodies

Other statutory bodies such as the Inland Revenue, Customs and Excise, DHSS, Department of Employment etc. If a request has come in from these departments or bodies all statutory information must be provided. In the event of an unusual request check with the Clerk.

(e) Other Local Authority / Public Bodies

Any request made by such bodies must be in writing and indicate the reason for requiring the data and the local authority and public body must have obtained the data subject's consent. Always ask for a copy of the written consent before disclosing any data.

(f) The Courts

Disclosures to Courts should only be made in relation to Court Proceedings or Orders etc. Do not disclose information that is not needed for such proceedings.

(g) Pensions

Disclosure should only be made to Leicestershire County Council if it relates to information required by it for the administration etc. Of the Superannuation Scheme.

(h) Trade Unions

In the case of trade unions, disclosure must only be made:

Where an employee is a member of the union and he or she had given the usual authority for deduction of union fees and the form giving authority to deduct should specify whether the employee consents to certain disclosures. For example, to official branch offices or authorised union representatives. In such cases the data/information disclosed must only relate to names, addresses and salary / pay as necessary to calculate the union fees due.

CARE MUST BE TAKEN SO AS NOT TO DISCLOSE PERSONAL DATA RELATING TO NON-UNION MEMBERS.

(i) Elected members

Disclosure must only be made by Members when acting in a capacity of a Member of the Council. Even when such disclosures are made it is prudent for Members to ensure that the data subject has given the appropriate consent. When a Member is

acting in the capacity of an agent, friend or on behalf of an employee, appropriate consent must be obtained.

(j) Disclosure to Members by Clerk

The Clerk must ensure that appropriate consent of the data subject is in place before disclosure of personal information to members.

(k) Authorised Staff

Information exchanged between different members of Staff in different departments should only take place when members of Staff are acting in the normal course of their duties. If there is any doubt as to whether disclosure is a normal requirement of the job description it is best to check with the Clerk. Unnecessary exchange of personal data should not be taking place between members of Staff.

(l) External Auditors of the Council

This covers the usual disclosures required for purposes of any audit.

(m) Security

(1) Terminals should be positioned where they can be kept secure by constant supervision and should not be positioned in such a way that the screen can be seen by unauthorised persons. Printers should be sited where they can be constantly supervised.
(2) Terminals must not be left unattended when 'signed on'. The user should log out and return the display to a menu scheme or switch off whenever the terminal is not in use.

(n) Systems

Passwords should be changed frequently and at irregular intervals. They should always be changed when an authorised password holder ceases to be so authorised. They should be chosen with care and those which could be easily guessed should be avoided.

Passwords should never be written down where they could be seen by unauthorised personnel.

(o) Output

Printed output should be accorded the same degree of security as data held on magnetic media. Confidential output, including output running instructions, file names etc, should be kept in a secure place.

Waste computer printout output media must be disposed with due regard for its sensitivity. Confidential and **personal** output should be destroyed by Shredding or other similar means.

Output should be disposed of as soon as it no longer serves any purpose. Care should be taken so that output which is ready for destruction is in fact destroyed and that any intermediate storage is secured.

(p) Back-up

Users should make regular copies of all of their files to the extent that recover can be effected without cost or significant delays. Each copy should be marked with the date on which it was taken. Back-up copies should be stored in a separate location.

(q) Manual Records

Access to and storage of manual records should be provided to reflect the level of confidentiality of the information held.

Output from and disposal / destruction of manual records should be undertaken in the same way as computer records.

SUMMARY OF PERSONAL RESPONSIBILITIES UNDER THE DATA PROTECTION ACT 1998

You should ensure that you:

(a) Do NOT allow unauthorised access to Personal Data.
(b) Do NOT without proper authority disclose Personal Data to others.
(c) Keep Personal Data secure so that it may not be lost, destroyed (even accidentally), or damaged.
(d) Keep Personal Data up to date and accurate.
(e) Remember that processing of certain sensitive data requires additional justification.
(f) Be careful what you send over the Internet or in the internal e-mail.
(g) Get consent from people before processing information about them.
(h) Consult the Clerk before you set up a new filing system, car system or computer system.
(i) Dispose of Personal Data in a secure manner.
(j) Check before you send Personal Data abroad.

Finally, failure to follow this guidance means the Council Members and Staff could personally face a claim for damages and distress that the data subject has suffered as a result and may in certain circumstances result in disciplinary action against the Staff including dismissal for gross misconduct.

This Policy was adopted by Thurcaston & Cropston Parish Council at the council meeting on 21st April 2016.