DESFORD PARISH COUNCIL

DATA PROTECTION POLICY

The Data Protection Act 2018 Six Principles of Good Practice

1. Personal data shall be processed fairly, lawfully and in a transparent manner.
2. Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in any manner incompatible with the purpose.
3. Personal data shall be adequate, relevant, and limited to what is necessary 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 shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were processed.
6. Personal data shall be processed in a manner that ensures security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using either technical or organisational measures.

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 given clear and explicit consent to process their personal data for a specific purpose.
2. The processing is necessary for a contract with the individual or before entering into a contract.
3. The processing is necessary to comply with the law.
4. The processing is necessary to protect someone's life.
5. The processing is necessary to perform a task in the public interest or for an official function when the task or function has a clear basis in law.
6. The processing is necessary for legitimate interests, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

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~~ philosophical beliefs, trade union membership, health condition, genetic data. biometric data for the purpose of uniquely identifying a person, sex life or sexual orientation.
Sensitive data can only be processed where:

1. The data subject has given explicit consent to the processing of their personal data for one or more specific purposes.
2. Processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law.

3. Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.
4. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject.
5. Processing relates to personal data which are manifestly made public by the data subject.
6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
7. Processing is necessary for reasons of substantial public interest.
8. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care systems and services.
9. Processing is necessary for reasons of public interest in the area of public health.
10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Guidance for Staff: The Data Protection Act 2018

The purpose of this statement is to provide guidance on the objectives of the Data Protection Act 2018 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 computers and 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 one month of the receipt of a properly completed application.

A person about whom information is held is, subject to any exemptions (see below) entitled to:

3.1 be informed by the data controller whether any information is held on them together with:
- (a) a description of the data
- (b) a copy of the information.

3.2 request and receive information giving:
- (a) the purposes for which the data is being held
- (b) the recipients or classes of recipients to whom it may be disclosed
- (c) the source of the data

3.3 restrict the processing of their data

3.4 object to the processing of personal data for direct marketing purposes.

3.5 not to be subject to automated decision making

3.6 receive compensation from the data controller and/or data processor for damage suffered as a result of an infringement of GDPR.

3.7 obtain from a data controller without undue delay the rectification of inaccurate personal data.

3.8 request that their personal data be erased by the data controller. (The further retention of data will be lawful in some cases.)

3.9 be notified by the data controller when a personal data breach is likely to result in a high risk to the data subject's rights.

3.10 Receive a copy of personal data or transfer personal data to another data controller.

Exemptions:
- (a) National security
- (b) Defence
- (c) Public security
- (d) The prevention, investigation, detection or prosecution of criminal offences.
- (e) Other important public interests (economic or financial interests including budgetary and taxation matters, public health and security).
- (f) The protection of judicial independence and proceedings
- (g) Breaches of ethics in regulated professions
- (h) Monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention.
- (i) The protection of the individual or the rights and freedom of others or
- (j) The enforcement of civil law matters.

4. Disclosure of Personal Data:

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

4.1 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.

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

4.3 New Employer of the Data Subject:

If a data subject's employer requests details, these should only be those relating to P45s and other statutory requirements. If anything beyond these requirements is sought, written authorisation or consent of the data subject must be obtained by the person requiring the information before information is disclosed to them by Desford Parish Council.

4.4 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.

4.5 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.

4.6 The Courts:

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

4.7 Pensions:

Disclosure should only be made to the pension provider if it relates to information required by it for the administration of the Superannuation Scheme.

4.8 Trade Unions:

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

Where an employee is a member of the union and they 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 eg. 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.

4.9 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.

4.10. 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.

4.11 Authorised Staff:

Information exchanged between different members of Staff 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.

4.12 External Auditors of the Council:

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

4.13 Security:

(a) Terminals should not be positioned in such a way that the screen can be seen by unauthorised persons. Personal information should not be left displayed on screen when not in use. Printers should be sited where they can be constantly supervised.
(b) 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.
(c) USB sticks should be filed away securely and not left lying around.
(d) If personal data is kept on a laptop or tablet, these should be securely stored when not in use.
(e) Workspace containing a computer or other device containing data should be locked when not in use.

4.14 Systems

Access should be by a unique password.
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 electronically. Confidential output, including output running instructions, file names etc should be kept in a secure place.

Waste computer printout output media must be disposed of 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 recovery 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. All personal data should be kept securely. Filing cabinets must be locked outside of normal working hours and keys held in the safe.

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 2018

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, card 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.

Adopted by Desford Parish Council on 20th March 2024