Barkestone, Plungar & Redmile Parish Council

Data Protection Policy

Provisions of Data Protection Act

The Data Protection Act 1998 has eight principles of good practice.

1. Personal data shall be processed fairly and lawfully & shall not be processed unless certain conditions are met.
2. Personal data shall be obtained only for one or more specified & lawful purposes & shall not be further processed in any manner incompatible with the purpose.
3. Personal data shall be adequate & relevant & not excessive in relation to the purpose for which they are processed.
4. Personal data shall be accurate & 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 with the rights of the data subject under this Act.
7. Appropriate technical & organisational measures shall be taken against unauthorised or unlawful processing or personal data & 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 & 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

Data Protection Policy in Practice at Barkestone, Plungar & Redmile Parish Council

The purpose of this section is to provide guidance on the objectives of the Data Protection Act 1998 & the obligations under the Act which apply equally to Parish Councillors & 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 Clerk may examine both computers or manual data to determine the accuracy of registration; Staff & Parish Councillors 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 & 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 will 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 & 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 & 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 etc Organisations and Agents of the Data Subject

   (c) New Employer of the Data Subject

   If a data subject's new employer, requests details, these should only be those relating to P45's & 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 Barkestone, Plungar & Redmile Parish Council.

(d) Other Statutory Bodies

Other statutory bodies such as the Inland Revenue, Customs & 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 that an unusual request is made check with the Clerk.

(e) Other Local Authority / Public Bodies

Any request made by such bodies must be in writing & indicate the reason for requiring the data. The local authority/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 the Parish Council's pension provider (if such a scheme has been agreed & set up by the Parish Council) if it relates to information required by it for the administration etc. of the Superannuation Scheme.

(h) Parish Councillors

Disclosure must only be made by Parish Councillors when acting in the capacity of a Parish Councillor. Even when such disclosures are made it is prudent for Parish Councillors to ensure that the data subject has given the appropriate consent. When a Parish Councillor is acting in the capacity of an agent, friend or on behalf of an employee, appropriate consent must be obtained.

(i) Disclosure to Parish Councillors by Clerk

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

(j) External Auditors of the Council

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

(k) Security

Laptop should be positioned where they can be kept secure by constant supervision & 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.

Laptops must not be left unattended when 'signed on'. The Clerk should log out & return the display to a menu scheme or switch off whenever the computer is not in use.

(l) Systems

Passwords should be changed frequently & 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.

(m) On-line Banking

The use of a personal identification number (PIN) and other password(s), for access to the council's bank accounts should be stored securely. A note shall be made of the PIN and Passwords and shall be handed to and retained by the Chairman of Parish Council in a sealed dated envelope. This envelope may not be opened other than in the presence of two other Parish Councillors. After the envelope has been opened, in any circumstances, the PIN and / or passwords shall be changed as soon as practicable.

Should the sealed envelope be opened, in whatever circumstances, this shall be reported to all Parish Councillors immediately and formally to the next available meeting of the Parish Council.

The Clerk shall not disclose any PIN or password to any person not authorised in writing by the Parish Council.

Access to any internet banking accounts will be directly to the access page (which may be saved under "favourites"), and not through a search engine or e-mail link. Remembered or saved passwords facilities must not be used on any computer used for council banking work.

(n) Printed Materials

Printed matter should be accorded the same degree of security as data. Confidential or sensitive papers, including file names etc should be kept in a secure place.

Printed materials must be disposed with due regard for its sensitivity. Confidential and personal output should be destroyed by shredding or other similar means.

Printed matter 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.

(o) Back-up

Documents are automatically saved to Cloud virtual storage.

(p) Manual Records

Access to & 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 other printed matter.

Personal Responsibility

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 & accurate.
(e) Remember that processing of certain sensitive data requires additional justification.
(f) Be careful what you send over the internet & in e-mails.
(g) Get consent from people before processing information about them.
(h) Consult the Clerk before you set up a new filing 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 Parish Councillors & Clerk could personally face a claim for damages & distress that the data subject has suffered as a result & consequently may in certain circumstances result in disciplinary action including dismissal for gross misconduct.

<u>Version Control</u>
Draft: reviewed by Parish Council 14 February 2017
Draft: review by Parish Council 16 May 2017
Adopted: 16 May 2017