HORDEN PARISH COUNCIL

DATA PROTECTION POLICY

Introduction

Horden Parish Council is committed to openness and accountability in the way that it carries out its work.

We will do what we can to ensure that the successful implementation of the Data Protection Act 1998 ("The Act"). This will enable us to serve our customers, stakeholders, and partners, elected members and the public more effectively and to build increasing levels of trust in the way that we carry out our responsibilities pertaining to the manipulation of personal data. It will also help to ensure that the services we provide are delivered efficiently and effectively.

This policy applies to all Council members and employees and provides a framework within the Council will ensure compliance with the Act and develop operational procedures to maintain adherence.

The Data Protection Act 1998

The Data Protection Act 1998 is "an Act to make provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal data". The Council will endeavour to apply the spirit of the Act to ALL data operations.

Horden Parish Council is required by law to collect and use certain types of information concerning individuals with whom it interacts to fulfil its statutory duties. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be dealt with properly however it is collected, recorded and used, whether on paper, stored electronically, or on other material

The overall responsibility for ensuring compliance with the Data Protection Act rests with the Clerk.

Policy Statement

Horden Parish Council will ensure that its treats personal information lawfully and correctly as this is essential in maintaining the confidence and operational efficiency between the Council and those with whom it carries out its business.

To this end the Council fully endorses and adheres to the 8 Principles of Data Protection as set out in the Data Protection Act 1998.

Data Protection Principles

The DPA states that anyone processing personal data must comply with the following eight principles of Good Practice, which are legally enforceable. The Principles require that personal information;

1) Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met.

2) Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

4) Shall be accurate and where necessary, kept up to date.

5) Shall not be kept for longer than is necessary for that purpose or those purposes.

6) Shall be processed in accordance with the rights of data subjects under the Act.

7) Shall be kept secure i.e. protected by an appropriate degree of security.

8) Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

In addition to the 8 Principles, Horden Parish Council will observe the following criteria to re-enforce good practice when the DPA applies;

1) Council staff managing and handling personal information is appropriately trained.

2) Council staff managing and handling personal information understands that they are contractually responsible for following good data protection practice and are fully aware of the Act and its implications.

3) A lead officer i.e. the Clerk is assigned with specific responsibility for the provision of data/information within the Council.

4) Council staff dealing with personal data and information is supervised accordingly and appropriately.

5) Regular audits are carried out on the way information is managed by the Council.

6) Information management processes are fully mapped and documented to provide clarity of purpose.

7) Records subject to the DPA will be retained and disposed of in accordance with the Councils Record Management Policy.

8) Take appropriate technical and organisational security measures to safeguard any personal information held.

9) Ensure the quality of the personal information used.

10) Collate and process information in an appropriate manner, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

11) Fully observe conditions regarding the fair collection and use of personal information.

Subject Access Requests

An individual may apply to obtain information by completing a Data Subject Access form which can be found on the Councils website or obtained by calling the Council on 0191 5180823.

There is a standard **£10 charge** that accompanies all subject access requests, which must be paid prior to the disclosure of the information requested.

The Data Protection Act gives an applicant; the "data subject" (a member of the public or a member of staff) the following rights:

Upon written application, access within **40 days** to information held by the council regarding their personal details. Under the DPA the data subject is also entitled to:

1) A description of the data being processed.

2) The purposes for which it is being processed.

3) A description of the recipients.

4) The source of the data where any decision is taken based solely on an automated process.

5) Upon written notice require the Council to cease or not to begin processing their personal data where processing is causing or likely to cause unwarranted substantial damage or distress to themselves or another. (the Council must respond within 21 days outlining the action proposed.).

6) Upon written notice require the data controller to cease or not to begin processing their personal data for the purposes of direct marketing, including disclosure to third parties for that purpose. (The Council must cease the processing within 28 days.).

7) Upon written notice require the Council not to take any decision, which significantly affects them that is based on automated decision taking.

8) Entitlement to compensation where an individual suffers damage and/or distress resulting from any contravention of the Act unless the Council can prove all reasonable care had been taken in the circumstances.

9) Right to apply for a court order requiring rectification, blocking, erasure or destruction of inaccurate personal data (including expressions of opinion based on inaccurate data), or of data processed in contravention of any provision of the Act where the subject is entitled to compensation from the Council and the court is satisfied that there is substantial risk of further contravention.

10) Right to require that third parties to whom inaccurate or contravening data has been disclosed be notified of the fact.

11) Ask the commissioner to assess whether or not processing of personal data is being carried out by the Council in compliance with the act if an individual has reason to believe they may have been adversely affected by the process of their data.

Conditions and Exemptions

When processing any personal data at least one of the following criteria must apply as disclosed in Schedule 2 of the Act);

1) The individual has given consent.

2) The processing needs to be done for the individual to enter into a contract, or to have a contract set up, or is necessary to comply with any legal obligation other than that imposed by contract;

3) The processing is necessary in order to protect the vital interests of the data subject.

4) Processing is necessary for the administration of justice, exercise of functions conferred under an Act of Parliament, exercise of functions of the Crown, or the exercise of other functions of a public nature in the public interest.

5) Processing is necessary for the legitimate interests of the Council, except where this may prejudice the rights and freedoms and legitimate interests of the data subject - this purpose may be regulated by specific orders of the Secretary of State.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data.

Personal data is defined as;

"*data relating to a living individual who can be identified from that data That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual"*.

There are additional requirements placed upon the Council where the holding of 'sensitive personal data' is concerned. Sensitive data is defined as;

- Racial or ethnic origin.
- Political opinion.
- Religious or other beliefs.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Criminal proceedings or convictions.

If sensitive personal data is held, security measures for holding such data must be considerably higher than that for other areas holding less sensitive data. In all cases where sensitive personal data is held, the Council must have a record of the justification and reasons for holding such data together with the procedures for ensuring confidentiality.

The rights of data subjects are subject to certain statutory exemptions. The Council will disclose personal information, without the data subject's consent in accordance with the DPA 1998.
This includes but is not limited to: -

1) On production of a court order for disclosure.

2) Where the purpose of disclosure is to enable the Authority to assess or collect any tax or duty or any imposition of a similar nature.

3) Where the purpose of disclosure would be to prevent or detect a crime, apprehend or prosecute offenders.

4) By order of the Secretary of State.

5) Where we are obliged by any law to disclose information.

6) Where information is required for research purposes providing such data is general and does not cause damage or distress to the data subject.

7) Where disclosure would be to safeguard national security.

8) To Elected Members, where disclosure is necessary to enable them to fulfill their statutory duties as a Councilor, i.e. for example where the Councilor is a member of a specific committee or when acting on behalf of a Constituent.

If a subject access request is refused, the Clerk must respond to the applicant in writing, within the e40 day deadline, clearly stating the reasons for refusal. They must also include a copy of the Councils appeals and complaints procedure.

Third Party Disclosure

Any request for data where received by a third party should be in writing and the third party must be identified. Where the third party relies on a legal authority for disclosure they must quote the relevant authority.

Unless an exemption applies, personal data will not be disclosed, except where the data subject consents to disclosure. Third party includes members of a data subject's family, legal representatives of a data subject, a data subject's employer and any body acting on behalf of an individual i.e. a Housing Association.

Requests for access from a third party should be accompanied by either an Authority to Disclose from the data subject or in the absence of this, necessary enquiries should be undertaken by the Clerk to ascertain if consent is given. If there is any doubt, written confirmation direct from the Data Subject should be sought.

The 40-day time limit also applies to requests for data from a third party, including the requirement to inform why a decision for not disclosing is made and the reasons for doing so. Again, this decision should be taken by the Clerk and the reasons for not disclosing documented and made clear to the third party. Nothing should be disclosed which would be likely to cause serious harm to a child's or vulnerable adult's physical or mental health. In all requests for access, the interests of the subject, particularly in the case of a child or vulnerable adult must be paramount and the duty of the Council to protect children and vulnerable adults from potential harm is of primary importance.

Elected Members

Councilors must ensure that Data Protection legislation and policy are complied with whatever role they may exercise. If the Member is in any doubt, they should contact the Clerk for clarification.

Where Councilors sit as the Council's representative on an outside body, the Councilor's duties will vary depending on the nature of the role taken but in the case of a Trustee or Director, they will owe a duty to the organisation on which they sit. In addition, Councilors are subject to the Code of Member Conduct, which includes duties in relation to information acquired or received in confidence.

Where the Councilor is required to act as Horden Parish Council's representative on other public sector bodies, joint boards, working parties etc, their status will be the same as if they were an employee of the Council. However, Councilors must not use their position as a representative to secure services for individual constituents. Conversely, Councilors must not pass on any personal information acquired as a Member to any outside body.

When Councilors are required to act as the Councils appointed representative on Local Government National Bodies, the Councilor's responsibility will be towards the body, which made the appointment and not the Council in the first instance.

If members are of a specific political party, Councilors will also be subject to any Data Protection conditions established by the organisation concerned. Councilors may in the course of their business seek to use personal data for their own purposes. This may include but is not limited to the following;

1) Constituency casework.

2) Where the Councilor is not carrying out their official duties but is acting in a personal capacity.

3) Canvassing political support.

4) Processing of personal duties held in connection with duties as a representative of a National Body.

5) Processing of personal data held and processed as part of the Councilors own business or profession.

If a Councilor is processing data for their own purposes they must ensure compliance with the principles of the DPA 1998. Councilors are also data subjects and as such, have the same entitlements as any other individual under the DPA 1998 regarding personal information held about them.

Disclosure to Elected Members

The Council does not always have to obtain the consent of the data subject for disclosure to the Member provided the Member represents the ward in which the data subject lives, in which case it is presumed that the Member acts on behalf of the data subject.

However, where disclosure is made of sensitive personal data, the consent of the data subject is required. Care must also be taken not to disclose anything which will

conflict with the needs of a child or vulnerable adult whose interests must be paramount i.e. child abuse investigations. Any information forming part of such court proceedings or investigation is highly unlikely to be able to be disclosed to a Member, even where the Member represents the ward in which the data subject lives. In addition, it is vital that information disclosed to Members is accurate and up to date.

The Clerk will determine in all cases what information is deemed acceptable to be divulged to members and may refuse inappropriate requests on the grounds of the DPA 1998.

When providing information to any Councilor, the Clerk should make a note of the request and make clear to the Councilor that the information is provided ***only*** for the limited purpose of assisting the data subject.

Where the information is requested by Elected Members for political purposes, consent of the individual data subject must be obtained except if the Council is required to make certain data public, i.e. lists of certain types of licence holders) or if information disclosed does not identify living individuals.

Generally, Elected Members are not treated as separate data controllers but are regarded as being within Horden Parish Council for the purposes of data protection. Where the Councilor receives personal data from the Council about individuals in order to enable them to carry out their statutory duties as a member of the Council, the Councilor's use of the data is subject to this policy as though the Councilor were an employee of the Council. Personal data will be treated as **confidential** and the requirements in respect of disclosure to third parties will apply.

Non-Compliance with Legislation and Policy

Horden Parish Council expects all employees to comply fully with this Policy, and the Data Protection Act 1998. Disciplinary action may be taken against any Council employee who knowingly breaches any instructions contained in, or following from this Data Protection Policy. Elected Members will be referred to Durham County Council's Standards Committee.

Individual employees are affected in the same way as the Council as a whole.

Anyone contravening the Act could be held personally liable and face court proceedings for certain offences which may result in a fine. If any of the principles of the Data Protection Act 1998 are breached, the data subject may be entitled to compensation and/or a decision may be made by the Information Commissioner or the Information Tribunal for their records to be amended.

The Information Commissioner or Information Tribunal may decide to uphold a decision of the Council following a decision not to disclose or amend information held. The Information Commission has power to investigate any aspect of a Data Controller's data processing of personal data and if need be, has powers to cause the processing to cease which would have catastrophic implications for the operational requirements of the Councils daily functions.

The Information Commission also has powers of entry and inspection into the premises of a data controller and in some circumstances has power to fine data controllers for an unlimited amount.

Further Information

For independent advice about data protection please contact the Information Commissioner at :

Wycliffe House
Water Lane
Wilmslow
Chesire
SK9 5AF
Website : www.informationcommissioner.gov.uk
Telephone 01625 545745
Fax 01625 524510
Email mail@ico.gsi.gov.uk