Driffield and Harnhill Parish Council
Privacy (Information & Data Protection) Policy

Introduction

In order to conduct its business, services and duties, Driffield and Harnhill Parish Council processes a range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

Driffield and Harnhill Parish Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Parish Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Parish community. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information Driffield and Harnhill Parish Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulation (GDPR) which became law on 25th May 2018 and will like the Data Protection Act 1998 before it, seek to strike a balance between the rights of individuals and the sometimes, competing interests of those such as the Parish Council with legitimate reasons for using personal information.
The policy is based on the premise that Personal Data must be:

• Processed fairly, lawfully and in a transparent manner in relation to the data subject.

• Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
• Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
• Accurate and, where necessary, kept up to date.
• Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
• Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Terminology

Data subject - means the person whose personal data is being processed. That may be an employee, prospective employee, associate or prospective associate of Driffield and Harnhill Parish Council or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person. It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Parish Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
• organising, adapting or altering it
• retrieving, consulting or using the information or data
• disclosing the information or data by transmission, dissemination or otherwise making it available
• aligning, combining, blocking, erasing or destroying the information or data, regardless of the technology used.

Driffield and Harnhill Parish Council processes personal data in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- monitor its activities including the equality and diversity of its activities.
- assist regulatory and law enforcement agencies
- process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- undertake research, audit and quality improvement work to fulfil its objects and purposes.
- carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time. The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any sensitive personal information and the Parish Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?

The Parish Council **as a corporate body has ultimate responsibility** for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Parish Clerk. Email: dhparishclerk@googlemail.com for full contact details.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data shall not be transferred to a country or territory outside the European Economic Areas 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.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Driffield and Harnhill Parish Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy. It is the responsibility of those individuals to ensure that the Parish Council is able to keep their personal data accurate and up to date. The personal information **will not be** shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Council's Right to Process Information: General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e). Processing is with consent of the data subject, or Processing is necessary for compliance with a legal obligation. Processing is necessary for the legitimate interests of the Council.

Information Security

The Parish Council cares to ensure the security of personal data. We make sure that information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. We will only keep data for the purpose it was collected for and only for as long as is necessary, after which it will be deleted.

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Rights of a Data Subject

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting our Parish Clerk.

Information Correction

If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate. Please contact: Parish Clerk.

Information Deletion

If the individual wishes the Parish Council to delete the information about them, they can do so by contacting the Parish Clerk.

Right to Object

If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Parish Clerk.

The Parish Council does not use automated decision making or profiling of individual personal data.

Complaints

If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Parish Clerk or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, and the website. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation on each Council and committee meeting.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated.

Minutes from all formal meetings are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council, but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure Information: The Council will as necessary undertake checks on both staff and Members with the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Data Transparency: The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

"Public data" means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery. The Code will therefore underpin the Council's decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:
Demand led: new technologies and publication of data should support transparency and accountability
Open: the provision of public data will be integral to the Council's engagement with residents so that it drives accountability to them.
Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance with which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Driffield and Harnhill Parish Council does not exceed this turnover and will ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillor or Member responsibilities
- Details of public land and building assets
- Draft minutes of Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

Personal data breach

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the person concerned must immediately notify the Clerk, or in their absence the Chairman
- The Clerk will investigate the report, and determine whether a breach has occurred. To decide, the Clerk will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Clerk will alert the Chair
- The Clerk will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant councilors or data processors where necessary.
- The Clerk will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Clerk and Chair together will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Clerk will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the Clerk must notify the ICO.

- The Clerk will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the Clerk will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Clerk will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Clerk
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the Clerk will report as much as they can within 72 hours.

The report will explain that there is a delay, the reasons why, and when the Clerk expects to have further information. The Clerk will submit the remaining information as soon as possible

- The Clerk will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Clerk will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the Clerk
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Clerk will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Clerk will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

The Clerk and Chairman will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Driffield and Harnhill Parish Council Review Date: Annually in May