Deopham & Hackford Parish Council
General Data Protection Regulation (GDPR) Policy and Privacy Notice

Adopted: 1 June 2018
Revised: 3 April 2024
Next review due: April 2025

General Data Protection Regulation (GDPR) Policy

Purpose of the policy and background to the General Data Protection Regulation
This policy explains to councillors, staff and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. This policy explains the duties and responsibilities of the council and it identifies the means by which the council will meet its obligations.

Identifying the roles and minimising risk
GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and the Parish Clerk (as Proper Officer) is the Data Protection Officer (DPO). It is the DPO's duty to undertake an information audit and to manage the information collected by the council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information. This is included in the Job Description of the clerk.

Appointing the Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.

GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the council (both financially and reputationally) and one which must be included in the Risk Management Policy of the council. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the council undertaking training in data protection awareness.

Data breaches
One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the Council (or individually appointed Councillors to the investigation). Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

Privacy Notices
Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information (Privacy Notice is available on the Council website). A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved.

Information Audit
The DPO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

Individuals' Rights
GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access

- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the Council to delete information.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The Council will be informed of such requests.

Children
There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the council requires consent from young people under 13, the council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

Summary
The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection will be included on the Council's Risk Management Policy.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

Privacy Notice

1. Background

This privacy notice lets you know what happens to any personal data that you give to us, or any that we may collect from or about you. It applies to all services and activities where we collect your personal data. This privacy notice applies to personal information processed by or on behalf of the Parish Council, as defined by the General Data Protection Regulation (GDPR) 2018.

Changes to this privacy notice

We may change this privacy notice from time to time by updating this page in order to reflect changes in the law and/or our privacy practices. We encourage you to check this privacy notice for changes whenever you visit our website.

The Parish Council and our Data Protection Officer

Deopham & Hackford Parish Council is the data controller of your personal data. The Parish Clerk (as Proper Officer) is the Data Protection Officer (DPO) who is responsible for data protection compliance. You can contact the DPO using the details below.

2. What kinds of personal information about you do we process?

Personal information that we will process includes:

- **Personal and contact details** (e.g. title, name, addresses, phone numbers)
- **Copies of correspondence between you and the Council** (e.g. emails you have sent us)

3. What is the source of your personal information?

We'll collect personal information from the following general source:

- From you

4. What do we use your personal data for?

We use your personal data, including any of the personal data listed in section 2 above, for the following purposes:

- To respond to a request for information
- To monitor and record our communications with you
- To comply with legal and regulatory obligations, requirements and guidance
- To assess job applications or to manage existing staff employment
- To process applications to become a councillor
- To carry out our public duties and tasks

We will never use your personal information for purposes other than those for which it was provided or obtained without first obtaining your consent.

5. What are the legal grounds for our processing of your personal information (including when we share it with others)?

We rely on the following legal bases to use your personal data:

- **Where it is needed to provide you with services**, such as processing requests for information or services that you make to the Council,
- To comply with our **legal obligations**
- For a **public task,** such as performing a task in the public interest or for our official functions, where the task or function has a clear basis in law
- With your **consent**, such as when you have given us clear consent to process your data for a specific purpose

6. When do we share your personal information with other organisations?

We may share information with the following third parties for the purposes listed above:

- Governmental and regulatory bodies, e.g. the District or County Council
- Other organisations and businesses who provide services to us such as back-up and email hosting providers, IT software and maintenance providers, document storage providers and suppliers of other back office functions
- Our bank – to make payments to you
- Our auditors

We have carefully selected these third parties to ensure they understand their obligation to put in place appropriate security measures and they will be responsible to you directly for the manner in which they process and protect your personal data.

7. How and when can you withdraw your consent?

Where we rely on your consent to process personal data, you can withdraw this at any time by contacting us using the details below, or via our website.

8. Is your personal information transferred outside the UK or the EEA?

We are based in the UK but sometimes your personal information may be transferred outside the European Economic Area. If we do so we'll make sure that suitable safeguards are in place, for example by using approved contractual agreements, unless certain exceptions apply.

9. What should you do if your personal information changes?

You should tell us so that we can update our records using the contact details below or via our website. We will then update your records if we can.

10. For how long is your personal information retained by us?

Unless we explain otherwise to you, we will hold your personal information based on the following criteria:

- For as long as we are required to in line with legal and regulatory requirements or guidance

- For as long as we have reasonable needs, such as managing our relationship with you and managing our work
- For as long as we provide services to you

11. What are your rights under data protection laws?

Here is a list of the rights that all individuals have under data protection laws. They don't apply in all circumstances. If you wish to use any of them, we'll explain at that time if they are appropriate or not.

- The right **to be informed** about the processing of your personal information
- The right to have your personal information **corrected if it is inaccurate** and to have **incomplete personal information completed**
- The right **to object** to processing of your personal information
- The right **to restrict processing** of your personal information
- The right **to have your personal information erased** (the "right to be forgotten")
- The right to **request access** to your personal information and to obtain information about how we process it
- The right to **move, copy or transfer your personal information** ("data portability")

You have the right to complain to the Information Commissioner's Office which enforces data protection laws: https://ico.org.uk/

Contact Us

If you have any questions about this privacy notice, or if you wish to exercise your rights or contact the DPO, you can do so via our website's Contact Us page or via email to deophampc@gmail.com. Alternatively, you can write to the Data Protection Officer at Deopham & Hackford Parish Council, 14 Gatekeeper Close, Wymondham, NR18 0XY.