

# **HARRINGWORTH PARISH COUNCIL**

## **DATA PROTECTION POLICY, PROCEDURES AND PRACTICES**

### **Statement of Commitment**

We understand the importance of ensuring that personal data, including sensitive personal data is always treated lawfully and appropriately and that the rights of individuals are upheld.

We are sometimes required to collect, use and hold personal data about individuals. Data is required for the purposes of carrying out our statutory obligations, delivering services and meeting the needs of individuals that we deal with. This includes current, past and prospective members of the Council, members of the public, our business partners and other local authorities or public bodies.

### **Policy Objectives**

In order to comply with the requirements of the General Data Protection Regulation (GDPR), we will ensure that:

1. Any personal data will be collected, used and held, lawfully and appropriately.
2. Regular data sharing with external partners and other relevant agencies will be subject to information sharing agreements. Partnerships will only be entered into where there is a clear statutory power enabling the council to participate.
3. The Clerk is the only appointed officer within the organisation who has specific responsibility, knowledge and requirement to hold individual data. He is the point of contact for all queries.
4. We will regularly review and update this policy, procedures and guidance for Council employees and Members.

### **Meeting our Policy's Objectives**

In order to meet the objectives that are listed above we need to ensure that the following are always considered and that appropriate controls and procedures are in place to ensure compliance with the General Data Protection Regulation (GDPR).

#### **Collecting and Processing Personal Data**

When we collect personal data we will ensure that where required, we make individuals aware that their information is being collected, the purpose for collecting the data specified, and whether it will be shared with any third parties. This will be done through the use of privacy notices. When reviewing documents and forms, we will always consider whether a privacy notice should be included.

#### **Data Security**

The Clerk must report any suspected data breaches to the Chairman for investigation and where necessary the Chairman will notify the Information Commissioner's Office. His report shall include the effects of the breach and the remedial action taken.

Council Members must use appropriate levels of security to share personal data.

An Information Asset Register will be maintained by the Clerk identifying:

- All personal data held
- where it is held
- how it is processed
- who has access to it

Personal data will not be shared with a third party organisation without a valid business reason and where required we will notify individuals that the sharing will take place in the form of a privacy notice. If any new purposes for the data sharing are to take place, we will seek consent from the individuals concerned.

When personal data is to be shared regularly with a third party, a Data Sharing Agreement must be implemented.

Any data sharing will also take into consideration:

- any statutory basis of the proposed information sharing
- whether the sharing is justified
- how to ensure the security of the information being shared.

### **Data Access**

Our employees and Members will have access to personal data only where it is required in order to fulfil their role.

All data subjects have a right of access to their own personal data;

Privacy Notices will include a contact address for data subjects to use should they wish to submit a Subject Access Request, make a comment or complaint about how we are processing their data, or about the handling of a Subject Access Request.

A Subject Access Request will be acknowledged to the data subject within 24 hours, with the final response and disclosure of information (subject to exemptions) within 30 calendar days.

A data subject's personal data will not be disclosed to them until their identity has been verified.

Third party personal data will not be released by us when responding to a Subject Access Request (unless consent is obtained, it is required to be released by law, or it is deemed reasonable to release).

### **Compliance with this Policy**

This Policy applies to all our Council Members and all people or organisations acting on behalf of the Council.

If any Council Member or persons acting on our behalf are found to knowingly or recklessly breach the Council's Data Protection Policy appropriate disciplinary and/or legal action will be taken.

Any questions or concerns about this policy should be taken up with our Clerk