Armitage with Handsacre Parish Council

GDPR Policy

Date created	Date adopted	Date last reviewed	Next review date
December 2024	December 2024	N/A	February 2025

Contents

1 INTRODUCTION

1.1. Many of the General Data Protection Regulations' (GDPR) main concepts and principles are the same as for the Data Protection Act 1998. However, there are also some new elements and enhancements meaning some things will need to be done differently.

1.2. The GDPR places greater emphasis on the documentation that the Council must keep to demonstrate its accountability. Compliance will require the Council to review its approach to governance and how it manages date protection including data sharing with other organisations.

1.3. The Information Commissioners Office (ICO) has produced a 12-point checklist on "steps to take now" which the Council will work through to ensure compliance.

2 AWARENESS

2.1 The Council will ensure that all Councillors and Officiers are aware the Law is changing.

2.2 The Council will work to identify areas that might cause compliance issues and use this to inform the Council's risk assessments.

3 INFORMATION HELD BY THE COUNCIL

3.1 The Council will undertake an information audit to determine what personal data it currently holds, where it came from and with whom it is shared.

3.2 The Council will maintain a record of its processing activities so as to comply with e-accountability principles within the GDPR.

3.3 The Council will ensure that any recording areas are corrected and that it notifies any organisation with whom it has shared such information.

4 COMMUNICATING PRIVACY INFORMATION

4.1 The Council will review its current privacy notices and priories any necessary changes so as to comply with the GDPR e.g. the lawful basis for processing data, the retention period and the individuals' right to complain to the ICO if they are concerned at how the Council is handling data.

5 INDIVIDUALS'' RIGHTS

5.1 The Council will review its procedures to ensure al the individuals' rights are covered including how the Council will delete personal data or provide data electronically and in a commonly used format.

5.2 The Council accepts the rights of individuals within the GDPR, namely:
- 5.2.1 The right to be informed;
- 5.2.2 The right of access;
- 5.2.3 The right of rectification;
- 5.2.4 The right of erasure;

5.2.5 The right to restrict processing;
5.2.6 The right to data portability;
5.2.7 The right to object; and
5.2.8 The right not to be subject to automated decision-making including profiling.

6 SUBJECT ACCESS REQUESTS

6.1 The Council will draft policy on how it will handle requests under the GDPR, for instance:

6.1.1 In most instances the Council will not be able to charge for complying with requests;
6.1.2 The Council will respond to requests within a month of receipt;
6.1.3 The Council may refuse or charge for a request where it is deemed to be manifestly unfounded or excessive;
6.1.4 The Council will inform the individual why it has refused and that they have the right to complain to the supervisory authority and to a judicial remedy.

7 LAWFUL BASIS FOR PROCESSING PERSONAL DATA

7.1 The Council will identify the lawful basis for its processing activity, document it and update any privacy notices accordingly.

8 CONSENT

8.1 The Council will review how it seeks, records and manages consent in order to ensure they meet the requirements under the GDPR.

8.2 The Council wil ensure that all consent is freely given; specific, informed and unambiguous, documents and can be easily withdrawn. Consent must be through a positive opt-in rather than inferred from silence, pre-ticked boxes or inactivity.

9 CHILDREN

9.1 The Council will review its systems for obtaining parental or guardian consent for any data it processes relating to children including the Youth Council.

9.2 The Council will ensure that any privacy notices relating to the collection of children's data is written in language that children will understand.

10 DATA BREACHES

10.1 The GDPR introduces a requirement on all organisations to notify the Information Commissioner's Office of certain data breaches which are likely to result in a risk of the rights and freedoms of individuals e.g. might lead to discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

10.2 Where the breach is likely to result in a high risk to the rights and freedoms of individuals then those concerned directly will also need to be informed.

10.3 The Council will establish procedures to ensure it is able to detect, report and investigate any personal data breaches.

11 DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS.

11.1 The GDPR males “Privacy by design” an express legal requirement.

11.2 The GDPR makes “Impact Assessments” mandatory in certain circumstances, for instance:

11.2.1 Where a new technology is being deployed;
11.2.2 Where a profiling operation is likely to significantly affect individuals; or
11.2.3 Where there is processing on a large scale of the special categories of data.

11.3 The Council will assess its processes to determine which, if any, circumstances exist where it might be necessary to conduct an Impact Assessment.

12 DATA PROTECTION OFFICER (DPO)

12.1 Under the terms of GDPR, an organisation must appoint a DPO with the appropriate knowledge, support and authority to take responsibility for data protection if it is:

12.1.1 A public authority;
12.1.2 An organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
12.1.3 An organisation that carries out the large scale processing of special categories of data, such a health records, or information about criminal convictions.

12.2 The ICO has confirmed that Local Council do not need to appoint a Data Protection Officer. Notwithstanding the ICO announcement, the Council will appoint the Deputy Clerk as the DPO and give them the authority and support to undertake this position. The DPO will report directly to the Full Council.