Alrewas Parish Council

General Data Protection Regulations

Approved Alrewas Parish Council GDPR Policy

1 Introduction

The General Data Protection Regulations (GDPR) became law in May 2018 and apply to the work of Alrewas Parish Council (the Council). All parish councils and other public bodies are required to have GDPR policies approved and published. There are significant legal and financial penalties for organisations which do not adhere to the requirements of the GDPR legislation.

In the case of any discrepancy between this document and the GDPR legislation, the GDPR legislation takes precedence over Council policy.

2 Purpose of this policy

This policy explains the duties and responsibilities of the Council and identifies the means by which the Council will meet its obligations.

Additionally, it is intended to enable Alrewas Parish Council to meet the requirements of GDPR legislation and to help councillors, employees and members of the public to understand such requirements in relation to the work and responsibilities of the Council.

3 Overview of requirements of GDPR

In outline, requirements of the legislation are:

Personal data must:

1. be processed lawfully, fairly and transparently
2. be collected for specified, explicit and legitimate purposes in relation to the work of the Council
3. be adequate, relevant and limited to what is necessary for processing
4. be accurate and kept current
5. be kept only for as long as is necessary for processing
6. be processed and disposed of in a manner that ensures its security, maintaining appropriate technical and security measures to protect personal data from loss, misuse, unauthorised access and disclosure.

4 Roles within the Council in relation to GDPR

All members of the Council are liable to GDPR regulations, must understand their responsibilities and will abide by this policy.

The Council is the Data Controller and will be represented by the Clerk in this role.

The Clerk will:

1. manage information collected by the Council
2. undertake an information audit
3. carry out procedures in relation to data collection, usage, storage and retention and deletion. These will include, but not be limited to issuing privacy statements, dealing with complaints and informing councillors of any changes to GDPR requirements

4. review policies annually for reapproval by the Council
5. Update the Business schedule document in relation to GDPR requirements

5 Risk and risk management

Monitoring of adherence to GDPR requirements and action on breaches is undertaken by the Information Commissioner's Office (ICO). The risks associated with not meeting GDPR requirements are HIGH in terms of reputation and financial penalty. The Council will manage GDPR so that the likelihood of such risk occurring is LOW. Penalties for a breach of regulations could include a fine and also compensation to any individual or group affected by a proven breach. To minimise risk the Council will:

1. Approve a GDPR policy compliant with national requirements
2. Undertake required activities, including
- An information audit and an annual review
- Issuing a privacy statement
- Developing and maintaining privacy impact assessments, including undertaking an audit of potential data risks associated with new projects
- Minimising access to sensitive information
- Developing a retention schedule and ensuring disposal of information
- Providing advice and guidance to councillors and employees
- Publishing relevant information, policies and guidance on the Parish Council website
- An annual review of GDPR policies and procedures with a report to the Council
3. Include GDPR requirements in the Risk Management Policy of the Council which will be monitored regularly by the Clerk and reported to the Council periodically
4. Provide guidance and information to all councillors and employees on the Council's policy and on GDPR requirements
5. Receive reports from the Clerk on any issues relating to GDPR, including any breaches
6. Review the GDPR policy annually to ensure that it continues to be compliant with national requirements and legislation

6 Information audit

The Clerk, on behalf of the Council, will undertake an Information Audit at least annually, or when a major initiative involving personal data is undertaken. The Information Audit should take place before an annual review of GDPR policies and outcomes minuted at the relevant Council meeting. The Information Audit will record the following:

- The personal data held
- Where it came from
- The purpose for holding the information
- With whom the Council will share the information

The Audit will cover electronic and hard copy information.

7 Collection of personal data

All data will be collected and processed by councillors and Council officers for the purpose of Council business only. The Council will only retain personal information as required for it to undertake its legitimate business. This includes, but is not limited to:

1. Personal detail of councillors while in office and for a year after they cease to be councillors. This may include, title and name, age, gender, marital status, nationality, work history, qualifications, family composition, financial identifiers

including bank account numbers, payment card numbers and other relevant details.

2. Information on employees, contractors etc as required for legal and financial purposes. This may include, address, telephone and e mail data, title and name, age, gender, marital status, nationality, work history, qualifications, family composition, financial identifiers including bank account numbers, payment card numbers and other relevant details.
3. Contact details of county councillors, district councillors and officers of these in such circumstances include, title and name, age, gender, marital status, nationality, work history, qualifications, family composition, financial identifiers including bank account numbers, payment card numbers and other relevant details.
4. Personal data held may also include sensitive material including criminal convictions, racial or ethic origin, mental health and other medical matters, political affiliations, and trade union affiliations. Sensitive material is described in GDPR legislation as "Special Categories of Data" which requires higher level of protection.
5. Planning information as held by Lichfield District Council, normally while planning applications are live and for three years after approval is granted. Data on larger or more complex applications may be held for longer as required at the appropriate time based on the retention schedule.

8 The legal basis for processing personal data

The Council is required under current legislation to process data to support its discharge of its statutory and legal functions. The Privacy notice sets out the rights of individuals whose data is processed.

9 Consent for collection of personal data

In limited circumstances the Council may approach individual for written consent to allow the Council to process certain sensitive data. In such circumstances full details will be provided of and the reason it is requested so than an individual can decide if they wish to release the data to the Council.

If information is collected on children or vulnerable adults then permission must be obtained from a parent, guardian or responsible adult. Children can give their own consent from the age of 13. Consent forms for children aged 13 plus must be written in easily understandable language.

10 Use of data

Data will be used for all or some of the following purposes which support the legitimate activities carried out by the Council:

- To enable the Council to meet all legal and statutory obligations and powers including any delegated functions
- To promote the interests of the Council
- To maintain the Council's records and accounts
- To carry out comprehensive safeguarding procedures
- To seek the views of residents
- To deliver public services including to understand the needs of individual and to advise on other relevant services as appropriate
- To confirm identity
- To contact individuals by post, leaflet drops, e mail, telephone or social media

- To help the Council monitor its performance
- To prevent and detect fraud and corruption in the use of public funds and where necessary, to support law enforcement
- Other activities relevant to Council business

11 Sharing of data

The Council may have to share personal data as it carries out its activities. Such third parties will be expected to comply with GDPR legislation.

12 Disposal of data

Data will be retained in line with the Retention Schedule.

Data will be disposed of securely. Electronic data will be deleted securely, in consultation with the Council's external IT advisor.

Paper based records will either be shredded in house or will be disposed of through an external secure shredding service, with certification of secure disposal obtained.

13 Data breaches

Personal data breaches should be reported to the Clerk, who will investigate on behalf of the Council. Investigations must be undertaken within one month of the report of a breach. The ICO must be informed within 3 days of a breach which is likely to result in a risk to the rights and freedoms of an individual. Where this risk is high the individual must be informed within 3 days by the Clerk acting on behalf of the Council.

Anyone linked to the Council, including councillors, officers and employees/contractors have a duty to use IT in a responsible way and to not disclose information about individuals to a third party. For example, discussion of internal council matters on social media is deemed unacceptable behaviour.

14 The rights of individuals in relation to personal date held by the Council
Individuals have the following rights under GDPR legislation:

1. The right to be informed of the data held on them
2. The right of access to the data
3. The right of rectification of the information held
4. The right of erasure of information held (the right to be forgotten)
5. The right to restrict processing
6. The right to data portability – the ability to move, copy or transfer data easily between different computers
7. The right to object to the data held or to the holding of date
8. The right not to be subject to automated decision-making including profiling
9. The right to complain to the Information Commission's Office (ICO) – see 16 below

Requests for changes to information should be made to the Clerk.

If a request relating to these rights is manifestly unfounded it can be refused or a charge made or processing. This will be detailed in the Council's Freedom of Information Publication Scheme. A decision on whether a request falls into this category will be made by the Clerk in consultation with the Council's GDPR working group.

15 Privacy notice

A privacy notice based on this policy will be published on the Council's website. Should date be required for a new purpose not listed in the Privacy Notice then revised information will be published on the Council website.

16 Transfers of date abroad

Any personal data transferred to countries or territories outside of the European Economic Area (EEA) will only be placed on systems with equivalent safeguards and protection of personal data. This will be confirmed by contracts issued by the EU or through international agreements.

The Council's website can be accessed from other countries and so data available to the public can be accessed, including contact details of councillors which are deemed public information for Council purposes.

17 Complaints

A complaint from an individual concerning the use of personal data can be made to the Parish Clerk, who will investigate on behalf of the Council in consultation with the GDPR working group. The outcome of any complaint will be reported to a full Council meeting.

Individuals have the right to complain directly to the Information Commission's Office (ICO) at:
The Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF

Phone: 0303 123 1113
E mail: https://ico.org.uk/global/contact-us/e-mail/

Website: https://ico.org.uk

18 Review of GDPR policy and procedures

The Clerk, on behalf of the Council, undertakes a review of GDPR policy and procedures on an annual basis. This will be in consultation with the GDPR working group. A report will be made to a full Council meeting which will approve any proposed changes. Any developments in legislation or accepted practice will be addressed by the Clerk and the GDPR working Group. Any recommendations will be approved by the Council and changes published on the Council's website.

Kathryn Powell
Clerk
March 2019
Reviewed April 2020
Reapproved May 2021