



Working with the community for the community

GDPR POLICY

INTRODUCTION

This document is the written policy of Kempley Parish Council regarding the protection of data and its use. The Council welcomes contributions from the community regarding the wording that has been adopted.

A Policy is not the same as the Standing Orders adopted by the Council.

This Policy was adopted or modified by the Parish Council:

Action	Date	Comment
Adopted:	19.07.18	For review at the Annual Parish Council Meeting
Modified:	06.11.18	Contents List Added
		Do's and Don'ts (Appendix 1) added
	21.11.22	Updated – for review at Ordinary Parish Council Meeting

Changes to this Policy

We keep this GDPR Policy under regular review and we will place any updates on the Council's website www.kempleyparishcouncil.org.

Contact Details

Please contact us if there are any questions about this GDPR Policy, the Data, or to exercise any relevant rights, queries or complaints at:

Kempley Parish Clerk
Phone: 07910842879
Email: clerk@kempleyparishcouncil.org

PERSONAL INFORMATION AND DATA (GDPR) POLICY

CONTENTS

No.	Description	Page
1.	The Data	2
2.	Kempley Parish Council	2
3.	Organisations or Individuals the Council works with	2
4.	The Council will acquire, hold and process the Data	2 & 3
5.	How the Council uses the Data where it is sensitive	4
6.	Does the Council need an individual's consent?	4
7.	The Council will comply with data protection law	5
8.	The purposes for which the Council may use the Data	5
9.	What is the legal basis for processing the Data?	6
10.	Sharing the Data	6
11.	Securing the Data	6
12.	How long does the Council store the Data?	7
13.	Rights and the Data	7 & 8
14.	Transfer of the Data Abroad	8
15.	Further processing	8

APPENDIX 1

Do's and Don'ts of GDPR

1. **The Data:**

“Personal information and data” is any information about a living individual which allows them to be identified, for example: a name, photograph video, email address, or residential address. Identification can be directly using the data or by combining it with other information to identify a living individual. Processing the Data is governed by legislation which applies in the United Kingdom including the General Data Protection Regulation (GDPR) and other legislation and rights such as the Human Rights Act.

2. **Kempley Parish Council:**

This Policy is provided by the Kempley Parish Council (the Council) who acquires, keeps and processes data and is therefore responsible for the security of it.

The Council, being a Parish Council, is not a Local Authority for the purposes of GDPR.

Do's and Don'ts guidance for councillors, the clerk and any person providing support to the Council are provided at Appendix 1.

3. **Organisations or Individuals the Council works with:**

The Council have had, or have a reasonable expectation to have contact with:

- Government bodies
- Local Authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Credit reference agencies
- Advisers to the above and members of the Community
- Individuals in the community
- Others, but only where reasonably necessary for the lawful purposes of the Council

The Council may need to share data with them so that it may exercise its statutory powers, obligations and duties. If the Council and the other data controllers or processors listed above are processing data jointly for the same purposes, then the Council and the other data controllers may be “joint data controllers” which means they and the Council are jointly responsible to an individual for their data. Where only one of the parties listed above is processing data for their own independent purposes they will then be independently responsible to an individual. If an individual has questions, wishes to exercise any of their rights (see Section 13 below) or wishes to raise a complaint, they should do so directly to the relevant data controller.

4. **The Council will acquire, hold and process the Data where reasonably necessary to perform its tasks. The Data may include:**

- Names, titles, and aliases
- Photographs
- Contact details such as telephone numbers, addresses, EMail addresses and physical location

- Data relevant to the services provided by the Council, or where an individual or organisation provides services to us
- Gender, age, marital status, nationality, education, employment, academic and professional qualifications, hobbies, family composition, and dependents
- Financial identifiers such as bank account numbers, payment card numbers, payment and transaction identifiers, policy numbers, and claim numbers
- Vehicles and other property
- Sensitive or other special categories of information such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, and data regarding sexual life or orientation
- Other information, but only where reasonably necessary for the lawful purposes of the Council

5. How the Council uses the Data where it is sensitive:

5.1 The Council may process sensitive personal data including, as appropriate:

- information about an individual's physical or mental health or condition or dietary requirements in order to monitor sick leave and take decisions on fitness for work or access or food requirements
- racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation
- in order to comply with legal requirements and obligations to third parties

5.2 These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. The Council needs to have further justification for collecting, storing and using this type of personal data.

5.3 The Council may process special categories of personal data in the following circumstances:

- In limited circumstances, with an individual's explicit written consent
- Where it needs to carry out our legal obligations
- Where it is needed in the public interest or the interests of the individual

5.4 Less commonly, the Council may process this type of personal data where it is needed in relation to legal claims or complaints, where it is needed to protect an individual's interests and they are not capable of giving their consent, or where they have already made the Data public.

6. Does the Council need an individual's consent to process sensitive personal data?

- In limited circumstances, the Council may approach an individual for their written consent to allow it to process certain sensitive personal data
- If it does, the Council will provide the individual with details of the Data requested and the reason for it, so that the individual may consider whether to consent

7. The Council will comply with data protection law. The Data must be:

- Used lawfully, fairly and in a transparent way

- Only for valid purposes and not used in any way that is incompatible with those purposes
- Accurate and up to date
- Kept only as long as necessary
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect it from loss, misuse, unauthorised access or disclosure

8. The Council may use the Data for the following purposes:

- To deliver public services including to understand the community's, an organisation's, or an individual's needs
- To provide the services that the community, an organisation, or an individual requests and to understand what the Council can do for them, and inform them of other relevant services
- To confirm an individual's identity to provide some services
- To contact an individual by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp)
- To help the Council to build up a picture of how it is performing
- To prevent and detect fraud and corruption in the use of public funds and where necessary for other law enforcement functions
- To exercise its Functions, including any delegated functions
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury
- To promote the interests of the Council
- To maintain our own accounts and records
- To seek the community's, an organisation's or an individual's views, opinions or comments
- To notify the community, an organisation or an individual of changes to our facilities, services, events and staff, councillors and other role holders
- To send communications which have been requested or that may be of interest to the community, an organisation or an individual. These may include information about campaigns, appeals, other new projects or initiatives
- To process relevant financial transactions including grants and payments for goods and services supplied to the Council
- To allow the statistical analysis of data so then Council can plan the provision of services
- Other purposes, but only where reasonably necessary for the lawful purposes of the Council

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

9. What is the legal basis for processing the Data?

The Council is a public authority and therefore processes the Data where reasonably necessary in relation to its Functions. However, the Council is not a Local Authority for the purposes of GDPR.

Data is processed in the discharge of its Functions. Sometimes it is necessary for the Council to process the Data of organisations or individuals using or contacting the Council regarding its Functions.

We may process the Data if it is necessary for the performance of a contract with an organisation or an individual, or to take steps to enter a contract. An example of this would be processing the Data in connection with an organisation in or related to the community or a community project, the Village Green, the bus shelters, or an Easement regarding them.

The Council will always consider an individual's interests and rights. This GDPR Policy sets out an individual's rights and the Council's obligations to them.

Sometimes the use of the Data requires an individual's consent. The Council will first obtain consent for that use.

10. Sharing the Data:

This section provides information about the third parties with whom the Council may share the Data. Those third parties have an obligation to put in place appropriate security measures and will be responsible to an individual directly for the manner in which they process and protect the Data. It is likely that the Council will need to share the Data with some or all of the following (but only where necessary):

- The data controllers or processors listed above under the heading "Organisations or Individuals the Council works with"
- The Council's agents, suppliers and contractors. For example, it may ask a commercial provider to publish or distribute newsletters on its behalf, or to maintain its database software
- On occasion, other local authorities or not for profit bodies with which the Council is carrying out joint ventures e.g. in relation to facilities or events for the community
- Others, but only where reasonably necessary for the lawful purposes of the Council

11. Securing the Data:

The Data are held in PC's, laptops, tablets, smartphones and similar electronic storage devices and their backup media used by the Clerk and Councillors. All such devices are required to be protected by relevant firewalls and access pin codes. In addition, the Clerk uses a lockable filing cabinet for hardcopy documents.

12. How long does the Council store the Data?

The Council will keep some records permanently if it is legally required to do so. It may keep some other records for an extended period. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. The Council may have legal obligations to retain some data in connection with its statutory obligations as a public authority. The Council is permitted to retain data to defend or pursue claims or complaints. In some cases, the law imposes a time limit for such claims, for example 3 years for personal injury claims or 6 years for contract claims. The Council will retain the Data for relevant purposes if it believes it is reasonably necessary to be able to defend or pursue a claim or complaint. In general, the Council will endeavour to keep the Data only for as long as it needs it. This means that the Council will delete data when it is no longer needed.

13. Rights and the Data:

An individual has the following rights with respect to the Data:

When exercising any of the rights listed below the Council may need to verify an individual's identity for security purposes. In such cases it will need an individual to respond with proof of identity before a right claimed can be exercised.

13.1 The right to access the Data relevant to an Individual

An Individual can contact the Council to request details of the Data relevant to them as well as why it has it, who has access to it and where the Council obtained it from. Once the Council has received a request it will respond within one month.

There are no fees or charges for the first request but additional requests for the same information or data, or requests which are manifestly unfounded or excessive, may be subject to an administrative fee.

13.2 The right to correct and update the Data

If the Data is out of date, incomplete or incorrect, an individual can inform the Council and the Data will be updated.

13.3 The right to have the Data erased

If an individual feels that the Council should no longer be using the Data relevant to them, or that the Council is unlawfully using that data, they can request that it be erased.

When the Council receives a request, it will confirm whether the Data has been deleted or the reason why it cannot be deleted (for example because the Council needs it for to comply with a legal obligation).

13.4 The right to object to processing of the Data or to restrict it to certain purposes only

An individual has the right to request that the Council stops processing the Data or ask it to restrict processing. Upon receiving a request, the Council will contact the individual and let them know if it is able to comply or if the Council has a legal obligation to continue to process the Data.

13.5 The right to portability of the Data

An individual has the right to request that the Council transfers some of the Data to another controller. The Council will comply with a request, where it is feasible to do so, within one month of receiving a request.

13.6 The right to withdraw consent to processing of the Data

An individual has the right to withdraw consent easily by telephone, email, or by post (see Contact Details below).

13.7 The right to lodge a complaint with the Information Commissioner's Office.

An individual has the right to contact, or complain to, the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. However, the Council would suggest an individual complains directly to it in the first instance (refer to the Council's Complaints and Comments Policy)

14. **Transfer of the Data Abroad:**

The Council's website is accessible from overseas and so some personal data (for example in a newsletter, agenda or minutes) may therefore be accessed from overseas.

The Council acknowledges that some servers are hosted abroad, for example Mailchimp in the US, so some data may be transferred to countries or territories outside the European Economic Area ("EEA").

15. **Further processing:**

If the Council wishes to use the Data for a new purpose, not covered by this GDPR Policy, then it will contact any relevant individual explaining the new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, the Council will seek an individual's prior consent to the new processing.

APPENDIX 1

Do's and Don'ts of GDPR:

- **Do** check that you have consent to share the Data
- **Do** check that you have an information sharing agreement in place
- **Do** think about the Data as if it were about you
- **Do** take care to protect laptops, devices and documents when taking them away from your workspace – keep them secure and under your control
- **Do** only hold the Data for as long as it is needed
- **Do** destroy files correctly and confidentially
- **Do** make sure you have correct and accurate data
- **Do not** share your passwords
- **Do not** leave your PC, laptop, device or filing cabinet accessible when away from it
- **Do not** leave documents on your desk if they contain personal or sensitive information
- **Do not** disclose or action requests to alter or delete personal information unless you are sure you have authority and you know who is making the request