Fakenham Magna Parish Council

Data Protection Policy

1 Introduction

1.1 To operate efficiently, Fakenham Magna Parish Council ('the Council') must collect and use information about people with whom it works. This may include members of the public, current, past and prospective councillors and employees, residents, contractors, suppliers, representatives of organisations and councils, job applicants and other stakeholders and individuals.

1.2 The Council regards the lawful and correct treatment of ***personal data*** as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business.

1.3 This policy outlines how the Council complies with the General Data Protection Regulation 2018 (GDPR) and subsequently revised UK Data Protection law in regard to the handling of personal data.

1.4 Fakenham Magna Parish Council is a ***data controller*** under the GDPR and has registered as such with the ***Information Commissioners Office (ICO).***

1.5 This policy describes how the Councillors, employees and role holders manage and protect personal data in the course of delivering the work of the Council. It covers the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to individuals.

2 Scope

2.1 This procedure applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, and film.

2.2 This policy is applicable to all councillors, employees, and role holders, and any partners, voluntary groups, third parties and agents authorised by them.

3 Personal Data collected by the Council

The categories of personal data that are collected by the Council include:

- Names, titles and photographs;
- Personnel details, e.g. staff start/leaving dates, education and work histories, academic and professional qualifications;
- Contact/client/customer/resident details, e.g. telephone numbers, addresses, e-mail addresses and electoral roll numbers;
- Where relevant to Council legal obligations or services delivered, or where individuals have provided them to the Council, demographic information, e.g. gender, age, marital status, nationality, family composition, and dependants;
- Financial information and identifiers in the context of contracts, purchasing and service agreements, e.g. bank account numbers, payment/transaction identifiers, policy numbers, VAT numbers, claim numbers, National Insurance numbers, pay and pay records, tax code, tax and benefits contributions, expenses claimed;
- Other operational personal data including but not limited to, planning applications, meeting attendees, logs of accidents, injuries and insurance claims;
- Recruitment information such as references and other information included in a CV or related documents;

- Other staff data including level, performance management information, information for disciplinary and grievance proceedings and personal biographies; and
- Councillor information, e.g. eligibility criteria, register of interests.

4 Personal Data Processing by the Council

4.1 All personal data processed by the Council will meet one of the five applicable lawful bases described in the GDPR (see Appendix A). This will be documented.

4.2 The Council will abide by the seven principles of data handling described in the GDPR (see Appendix A), and will use them to determine future data handling requirements

4.3 When processing 'Special Categories' of personal data (see Appendix A), the Council will identify both a lawful basis (as described in 4.1 above) and a permitted exemption to the general prohibition of processing such data stipulated by the GDPR**.**

5 Responsibilities of the Clerk

Whereas all councilors, role holders and staff are accountable for ensuring compliance with this policy, the Clerk to the Council has additional responsibilities for assisting the Council to monitor compliance with the legislation, and all relevant procedures. Their duties include:

- Keeping the Council and councillors updated about data protection generally including responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Keeping up-to-date with the legislation and issues affecting parish councils
- Answering questions and queries on data protection from requesters e.g. councillors, residents, other authorities, the ICO, and providing prompt and appropriate responses to subject access requests.
- Ensuring all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Approving data protection statements attached to e-mails, Council pages on the Website, correspondence and similar.
- Monitoring the implementation of and compliance with policies, procedures and the GDPR in general.
- Advising the Council on the data protection implications of any new projects or initiatives. The Clerk will be responsible for conducting any privacy impact assessments and ensuring that all appropriate projects commence with and include a privacy plan which is then maintained throughout the project lifecycle**.**
- Recommending to the Council any changes to its Risk Register and governance arrangements in the context of data protection.
- Carrying-out data protection audits.

6 Data Security and Storage

6.1 The Council will adopt physical, technical, and organisational measures to provide for the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of, in particular, human action or the physical, technical or natural environment. Measures will include the following:

- when data is stored on printed paper, it will be kept in a secure place where it cannot be accessed by unauthorised personnel;
- printed personal data will, as necessary, be shredded when it is no longer needed;
- personal data stored on a computer will be protected by strong passwords that are changed regularly;
- personal data will not be stored on portable media, e.g. CDs, memory sticks;

- personal data will be regularly backed-up on external hard drives held by the Clerk or a suitable secure cloud;
- personal data will not be saved directly to mobile devices such as tablets or smartphones.

7 Equipment Security and Passwords

7.1 Councillors and officers are responsible for the security of the equipment allocated to them, and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be set on all IT equipment and passwords must remain confidential and be changed regularly.

7.2 Users must only log onto Council systems using their own username and password. Users must not use another person's username and password or allow anyone else to log on using their username and password.

7.3 Councillors and officers using their own devices shall have the following responsibilities:

- Users will not use their device to store Council personal data or Council files containing personal data.
- Users will ensure council e-mail threads are copied or blind copied to the clerk. Once dealt with, the e-mails will be deleted from their device.
- Users will ensure security software is set up on their device and kept up to date.
- Users will enable their device is password protected.
- Users will inform the Council should they lose their device.
- Users will ensure that when they sell, recycle or discard their device, the hard drive is either wiped clean of all data or removed and destroyed.
- Users will not lend their device to any unauthorised person.

8 Systems and Data Security

8.1 Users should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

8.2 Users must not download or install software from external sources onto hardware owned by the Council. Downloading unauthorised software may introduce viruses or other malware.

8.3 Users must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to Council owned computers unless it has been authorised by the Council.

8.4 Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

9 Data Retention

9.1 To ensure fair processing, the Council will not retain personal data for longer than is necessary in relation to the purpose(s) for which it was originally collected, or for which it was further processed. What is necessary will depend on the circumstances of each situation, taking into account the reasons that the personal data was obtained, but will be determined in a manner consistent with legal obligations and Council data retention guidelines.

9.2 The length of time for which the Council needs to retain personal data is set out in the Records Retention Policy (FM-025).

9.3 All personal data will be securely and safely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

10 Data Audit, Personal Data Register and Risk Register

10.1 To confirm that an adequate level of compliance is being achieved by the Council in relation to this policy, the Clerk will carry out an annual data protection compliance audit and report on that audit to the Council.

10.2 The audit will be used to identify and manage risks, and will be used to inform both the Council Risk Register and Council Register of Personal Data. The latter contains information on what data is held, where it is stored and for how long, how it is used, and who is responsible for it.

11 Reporting Personal Data Breaches

11.1 A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. The process to be followed in the event of a personal data breach is described in FM-024 Personal Data Breach Procedure.

12 Individual Rights

12.1 When an individual seeks to exercise any of their rights (see Appendix A), for example to modify or erase data, the Council may need to verify their identity prior to processing the request.

12.2 Written requests received from individuals will be directed to and dealt with by the Clerk who will log each request as it is received and ensure a response at the earliest opportunity and certainly within one month from receipt.

12.3 To exercise their ***'right of access'***, an individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR).

13 Subject Access Requests

13.1 Individuals can make a Subject Access Request to find out:

- what personal information the council holds about them
- how the council are using the information;
- who the council are sharing it with; and
- where they got the data from.

Information on how an individual can make a SAR can be found in the privacy notices. Subject Access Requests received by the Council are handled by the Clerk following the procedure described in FM-023 Subject Access Request Procedure.

14 Privacy Notices

14.1 Privacy Notices describe how the Council uses personal data, and what rights individuals (data subjects) have in relation to that data.

14.2 A Privacy Notice will be supplied at the time personal data is obtained, if obtained directly from the data subject. Otherwise the Privacy Notice will be provided within a reasonable period of having obtained the data, and certainly within one month.

14.3 The Council has two separate privacy notices, one for internal use (specific to staff and councillors, former councillors and role holders) and one for external use (for customers, residents, suppliers etc).

15 Further Processing

15.1 If the Council wishes to use previously collected personal data for a new purpose, then the lawful basis should be redetermined, and the privacy notice updated to include the relevant purposes and processing conditions. Consent should be sought prior to the new processing.

15.2 A new lawful basis may not be needed provided that the new purpose is compatible with the original purpose, although this does not apply to processing based on consent. Accordingly, the Council will either seek fresh consent which specifically covers the new purpose, or find a different basis for the new purpose. Further details on determining the compatibility of old and new purposes can be found on the ICO website.

15.3 There are some limited circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. The GDPR specifically states that further processing for the following purposes should be considered to be compatible lawful processing operations:

- archiving purposes in the public interest
- scientific research purposes
- statistical purposes

16 Sharing Information

16.1 The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

16.2 Information will always be shared in a secure and appropriate manner and in accordance with the information type.

16.3 Any Councillor or officer dealing with telephone enquiries must be careful about disclosing personal information held by the Council. In order to manage this the enquirer will be asked to put their request in writing in the first instance.

16.4 The Council will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient.

17 Failure to Comply

17.1 The Council is fully committed to compliance with this policy and any failure in that regard will be viewed as extremely serious given that such failure, by a councillor or member of staff, may put both the individual and the Council at risk.

17.2 Failure to comply may lead to disciplinary action against staff, a councillor breaching the Suffolk Local Code of Conduct, a formal complaint by a data subject which may lead to action by the ICO and possible fine, and reputational damage to the Council.

Appendix A

1. Data Protection Principles

There are seven principles of data handling in the GDPR, they are:

- **Lawfulness, fairness, and transparency** - Using data in a way that complies with the law, that people expect and have been told about.
- **Purpose limitation** – only using personal data for the reasons it was collected and not for something extra or unrelated.
- **Data minimisation** – limiting the amount of personal data the Council collects to what it needs.
- **Accuracy** – keeping the personal details in the Council's records should accurate and up to date.
- **Storage limitation** – only keeping personal data for as long as the Council needs it. When it is no longer needed , the data should be securely destroyed or deleted.
- **Integrity and confidentiality (security)** – keeping personal data securely. Protecting the details of your staff and customers and that you can access those details.
- **Accountability** – this underpins the other six principles. It's about taking responsibility, having appropriate measure in place, and keeping records to demonstrate how data protection compliance is achieved.

2. Lawful Basis for Processing

There are five applicable lawful for processing data, they are:

- **Consent:** the individual has given clear consent for the Council to process their personal data for a specific purpose. Consent requires 'clear affirmative action'. Where the Council relies on consent as the lawful basis for processing any personal data, it will only do so where that has been freely given, is specific, informed, unambiguous and able to be withdrawn. As appropriate, it will record how and when the consent was obtained. Signed copies of consent forms will be collected with the issue of general Privacy Notices.

  For councillors and staff, the Council will not rely on consent because consent must be freely given. As it is necessary to process certain personal data for councillors and staff to allow them to perform their roles, and the balance of power between them and the Council is unequal, consent cannot be said to be 'freely given'. Thus, councillors and staff will not need to sign consent forms but will need to be issued with Privacy Notices.

- **Contract:** the processing is necessary for a contract the Council has with the individual, or because they have asked the Council to take specific steps before entering into a contract.

- **Legal obligation:** the processing is necessary for the Council to comply with the law (not including contractual obligations).

- **Vital interests:** the processing is necessary to protect someone's life.

- **Public task:** the processing is necessary for the Council to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

3. Individual Rights

The following rights of individuals are described in the GDPR:

- **The right of access to personal data**
  An individual can request to know what personal data the Council holds on them as well as why the Council holds that data, who has access to the data and where the data was obtained from. The Council will respond to requests within one month.

- **The right to correct and update personal data**
  An individual can request the Council to update the data it holds on them if it is If the data we hold on you is out of date, incomplete or incorrect.

- **The right to have personal data erased.**
  If you feel we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data that we hold. When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted.

- **The right to object to the processing of personal data, or to restrict it to certain purposes only.**
  You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you to let you know if we are able to comply or if we have a legal obligation to continue to process your data.

- **The right to data portability**
  You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

- **The right to withdraw consent to the processing at any time for any processing of data to which consent was obtained.**
  Individuals can withdraw their consent to data processing at any time.

- **The right to lodge a complaint with the Information Commissioners Office.**
  Individuals can complain directly to the ICO about data processing.

4. **'Special' Categories of Personal Data**

4.1. Several categories of data need to be treated with greater care because collecting and using them is more likely to interfere with the fundamental rights of individuals or open someone up to discrimination. The special categories are:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

4.2. The GDPR prohibits the processing of these special categories of data, but allows for certain exemptions. So, to process any data in these special categories the Council will establish both a

lawful basis (Section 2) and an applicable exemption. The exemptions are listed on the ICO website.

Glossary

Personal data is defined as any information, including opinions and intentions, which relates to an identified or identifiable natural (living) person, e.g. name, e-mail address.

A **data controller** is defined as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processing includes anything done with/to personal data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Information Commissioners Office (ICO). The ICO are the independent public authority responsible for monitoring the application of the relevant data protection regulation set forth in national law