Fakenham Town Council

Data Protection Policy

Adopted: Meeting of the Full Council, March 2021

To be reviewed annually/date of next review March 2022

Purpose of the policy and background to the General Data Protection Regulation

This policy explains to Councillors, Staff and Public about GDPR. Personal data must be processed lawfully, fairly and transparently, collected for specified, explicit and legitimate purposes, be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy updates any previous data protection policy and procedures to include the additional requirements of GDPR which apply in the UK from May 2018. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement. This policy explains the duties and responsibilities of the council and identifies the means by which the council will meet its obligations.

Most relevant data protection legislation for the town council

- Data Protection Act (DPA) 2018
- General Data Protection Regulation (GDPR)
- Freedom of Information Act (FOIA) 2000
- Environmental Information Regulation (EIR) 2004

Definitions:

Personal Data

- There are two general categories of personal data from a legal point of view:
  - basic (non-sensitive) information, typically normal contact details
  - special category (previously referred to as sensitive data). Examples of special category data include information relating to health, racial or ethnic origin, political opinions, religious beliefs, and genetic and biometric data when used to identify someone. Processing of special category data is prohibited unless the controller has identified a lawful basis and meets one of the conditions set out in Article 9 of the GDPR. Additional safeguarding measures (technical and organisational) must be put into place with associated proof of activity and processes subject rights.
- Privacy: Enshrined in law – see Article 8 of the Human Rights Act 1998 which states that: 'Everyone has the right to expect privacy for his private and family life, his home and his correspondence' but this is a qualified right i.e. with exceptions.
- Confidentiality: Is an agreement between 2 or more parties based on keeping certain information secret or limited to specific people.
- Data Protection: Legislation dominated by a set of principles and rights.

The GDPR require that personal data shall be:
• processed lawfully, fairly, and transparently
• collected for specified, explicit and legitimate purposes
• adequate, relevant and limited to what is necessary
• accurate and, where necessary, kept up to date
• kept for no longer than is necessary
• processed in a manner that ensures appropriate security

Identifying the roles and responsibilities

GDPR requires that everyone within the Council must understand the implications of GDPR and that roles and duties must be assigned.

The Council is the Data Controller whose duty it is to undertake an information audit, to manage the information collected by the Council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.
The Data Controller must respond to a data subject's request to exercising a right within one calendar month.
• Ordinarily, the controller cannot charge a fee to fulfil the request
• All the rights are qualified, do not apply in all circumstances but, if denied, the controller must explain why.
• The most likely request will probably be a data subject access request (DSAR) where the controller provides information relating to the data subject in a concise, transparent, intelligible and easily accessible form using clear and plain language appropriate to the requester.

Data Protection Officer (DPO)
Under Data Protection Act 2018 Section 7(3) Fakenham Town Council is not a public authority so is exempt from appointing a DPO. However, the Council will appoint a DPO as and when required from a list of suitably qualified data protection consultants maintained by the Clerk.

The Clerk and Deputy Clerk will be the data processors.

GDPR requires continued care by everyone within the Council, both Councillors and Staff, in the sharing of information about individuals, whether as a hard copy or electronically.

Councils must ensure the confidentiality, integrity and availability of all personal data they hold, even if the data is being processed through personal email accounts or is stored on a privately-owned device. Although such devices are privately owned, the council related information is not. Councillors could be asked to provide the content of messages or other information in the event of a subject access request or a request under the FOIA and/or the EIR.

A breach of the regulations could result in the Council facing a penalty from the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the Council (both financially and reputationally) and one which must be included in the Risk Management Policy of the Council. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with

new projects), minimising who holds data protected information and the Council undertaking training in Data Protection awareness.

Six Steps for Data Sharing

- Be clear about your purposes; There must be a specific purpose for sharing personal data. Check the sharing is necessary. The sharing has to be more than just useful or standard practice for it to be necessary.
- Identify your lawful basis; To comply with GDPR you must identify and document an appropriate lawful basis for sharing the information.
- Only share the personal data you need to; Councils should only share the minimum amount of personal data that is needed to help your council achieve its purpose.
- Inform individuals about the data sharing; Individuals have a right to be informed about the use of their personal data.
- Demonstrate your accountability: The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles of GDPR.
- Documenting the purposes and lawful bases for your council's data sharing is a good example to demonstrate your accountability.
- If you regularly share data with the same organisation, then a data sharing agreement would be good practice to demonstrate your accountability.

Rights of Individual's

NB: GDPR does not cover processing of personal data which concerns legal persons (such as limited companies). There is no regulatory requirement to redact the name, form or contact details of the legal person.

• Right to be informed as to how your personal data is being processed – this is normally done through a fair processing notice or privacy statement

• Right to access your personal data which is done by making a 'Data Subject Access Request' (DSAR)

• Right to rectification of your personal data if you believe it has been collected incorrectly or it needs to be updated

• Right to erasure of your personal data for which an organisation no longer has a lawful basis to process or where your interests override those of the data controller

• Right to restrict processing under certain circumstances, during which time your personal data but will be out of operational use until the related matter is resolved

• Right to data portability of your personal data in a machine-read able version but only applicable to data provided with your consent or under contract

• Right to object to the processing of your personal data for which there is not a legal or contractual obligation, typically associated with direct marketing

• Rights related to automated decision making and profiling where you have the right not to be subject to decision based solely on automated processing, including profiling, which produces legal effects or similar significant impacts

Data breaches

Procedures are in place to detect, report and investigate a personal data breach. Personal data breaches should be reported to the Clerk who will consult with the Data Protection Sub Committee about the appointment of a DPO. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals; if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. With the support of the Data Protection Sub Committee the DPO will undertake the investigations within one month of the report of a breach, where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.
It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and Councillors to use IT in any way that may cause problems for the Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

Privacy Notices

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information. A privacy notice will contain the name and contact details of the data controller, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. The issue of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved.

Information Audit

The Clerk must arrange with the Data Protection Sub Committee for an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy.
Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

If a request is received to delete information, then the Data Controller must respond to this request within a month.

If a request is considered to be manifestly unfounded the request could be refused or a

charge may apply. The charge will be as detailed in the Council's Freedom of Information Publication Scheme. The Data Protection Committee will be informed of such requests.

Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the council requires consent from young people under 13, it must obtain a parent or guardian's consent in order to process the personal data lawfully.
Consent forms for children aged over 13 must be written in language that they will understand.

Summary

The main actions arising from this policy are:

- The Council must be registered with the ICO.
- This policy will be considered as a core policy for the Council and be available on the website.
- An information audit will be conducted and reviewed annually or when projects or services change.
- A Privacy Statement will be displayed on the Council website.
- Appropriately worded Privacy notices must be issued.
- Data Protection will be included on the Council's Risk Management Policy.
- The Policy & Resources Committee will appoint a Data Protection Sub Committee (3 members with formal training and clear terms of reference) to manage the above processes.
- The Council will maintain a list of potential DPOs, who have agreed to be available, which will be reviewed and confirmed annually.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality, and the interests of the Council.

Reviewed at Policy & Resources Committee March 2021
Ratified at Full Council March 2021