Freckenham Parish Council
General Data Protection Regulation Policy

Purpose of this policy

This policy explains to councillors, staff and the 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 it identifies the means by which the council will meet its obligations.

Identifying the roles and minimising risk

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

The Clerk /RFO is the Data Processor.

The Data Protection Officer (DPO) is the Clerk/RFO.

It is the Data Processors' duty to undertake an information audit and to manage the information collected, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information. This will be overseen by the DPO.

GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the council facing a fine 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 which forms part of our Data Audit 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.

Information Audit

The Data Controller must undertake 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.

Privacy Notices

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the 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. Issuing of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt privacy notices which will be tailored depending on the person.

Data breaches

One of the duties assigned to the DPO is the investigation of any breaches. Personal data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the Parish Council.

Investigations must be undertaken within one month of the report of a breach.

If a personal data breach is detected. The ICO will be advised of a breach (within 3 days) and the DPO will call an emergency meeting to determine the correct procedure to rectify the breach.

Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

If a request is received asking for information held on them and/or delete the information held, the DPO will call an emergency meeting to determine the correct procedure to carry out and must respond to this request within a month.

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, the council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

Storage of Data

In order to keep any data held stored safely the Data Controller must ensure:

- Personal Data will be held by the Data Processor at their home address and will not be visible to the public from outside the home
- All data and council files to be backed up once a week onto a USB stick which is to be stored separately to the computer
- The device in which data and files are kept is to have adequate anti-virus software
- All data and council files are to be backed up to a USB stick once a week (to be held separately from main device), backup software once a week and cloud storage once a month
- Any devices used to access emails containing council business must be password protected

Summary

The main actions arising from this policy are:

• The Council must be registered with the ICO.
• A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
• An information audit will be conducted and reviewed at least annually or when projects and services change.
• Privacy notices must be issued.
• Data Protection will be included on the Council's Risk Management Policy which forms part of the Data Audit.
• The Parish Council will manage the process.

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.