Tattersett Parish Council

Data Protection 2018
Policy

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

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 came into force in the UK with the passing of the Data Protection Act in May 2018. This policy explains the duties and responsibilities of the council and it identifies the means by which the council will meet its obligations.

It was adopted on 20.07.20 and will be reviewed every third year unless the law requires otherwise.

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 and the clerk is the Data Protection Officer (DPO). It is the DPO's duty to undertake an information audit and 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 personal information. This will be included in the Job Description of the clerk.

Appointing the Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.

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 of the council. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (for areas of high risk - such as the installation of CCTV), minimising who holds data protected information and the council undertaking training in data protection awareness.

The public will be informed about Data Protection through the Council's website on which will be this policy, a general notice about data protection and a Privacy Statement.

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 an appointed Committee / Working Party. Investigations must be undertaken within one month of the report of a breach. Procedures are in place to detect, report and investigate a personal data breach.

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. 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. It is unacceptable for individuals to be named at either council meetings or in council minutes or in correspondence.

Privacy Statement

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the GDPR. The most common way to provide this information is in a privacy statement. This will be easily accessible on the Council's website. This is a notice to inform individuals about what a council does with personal information. It will contain the name and contact details of the data controller and DPO, 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. Reference to the privacy statement must be detailed on the Information Audit kept by the council.

Information Audit

The DPO 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. When councillors receive e mails from residents they should be forwarded to the DPO for inclusion on the information audit. The DPO will respond to the e mail and direct the person to the privacy statement on the website.

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 to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the Council to delete information.

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.

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, and will be reviewed annually / as the law requires.
- The Clerk's Contract and Job Description (as DPO) will be amended to include additional responsibilities relating to data protection.
- An information audit will be conducted and reviewed at least annually.
- The Parish Council website will have a privacy statement and general DP information which is easily accessible to the public.
- The process will be managed by the DPO reporting to the Parish Council.

This policy document is written with current information and advice.

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. The Council will maintain a training budget to support staff and councillors with this matter.