Ettington Parish Council

General Data Protection Regulations Policy and Process

Date Adopted: May 2018

Reviewed: May 2023 230510/5

Purpose of the Policy and Background to the General Data Protection Regulations

1.1 This policy explains to councillors, staff and the public about GDPR.

1.2 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.

1.3 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.

1.4 The Government have confirmed that despite the UK leaving the EU, GDPR will still be a legal requirement.

1.5 This policy explains the duties and responsibilities of the council and it identifies the means by which the council will meet its obligations.

1.6 The GDPR has six principles which are:

- **Fair Process:** Processed fairly, lawfully and in a transparent manner in relation to the data subject;
- **Collected for specific, explicit, legitimate purposes** and not processed further for purposes incompatible with those purposes
- **Adequate, relevant** and limited to what is **necessary**
- **Accurate** and, where necessary, **up to date**
- **Kept** in a form that permits identification of data subjects for **no longer than is necessary** for the purpose for which the personal data is processed
- Processed to ensure **appropriate security** including protection **against unauthorised or unlawful processing** and against **accidental loss, destruction or damage**

2 **Identifying the Roles and Minimising Risk**

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

2.2 The Council is the data controller and the clerk is the Data Protection Officer(until such time as there is clarity on the requirements of this role) (DPO).

2.3 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 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.

2.4 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 high / 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.

3 Data Breaches

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

3.2 The ICO will be advised of a breach within 72 hours 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.

3.3 It is unacceptable for employees, volunteers and members 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.

4 Privacy Notices

4.1 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 and Data Protection Officer, 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 a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

5 Information Audit

5.1 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. 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.

6 Individuals' Rights

6.1 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.

6.2 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.

6.3 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.

6.4 If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The charge will be as detailed in the council's Publication Scheme (FoI). The council will be informed of such requests.

7 Children

7.1 There is special protection for the personal data of a child. The age when a child can give their own consent, for the purpose of this policy, is 13. If the Council request 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 aged 13+ must be written in language that they will understand.

8 Summary

The main actions arising from this policy are:

- The Council must be registered with the ICO (it is)
- A copy of this policy will be available on the Council's website.

- The Clerk's Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.
- 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 in the Council's Risk Assessment

This policy is written with current information and advice. It will be reviewed at least annually or when further advice is issued/legislation changes.

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.

9 Procedure in Respect of Data Subject Access Requests

9.1 Data Subject Access Requests should be addressed to the clerk in writing by post or e-mail to:

Epc.clerk@yahoo.com
Clerk to Ettington Parish Council
PO Box 6271
STRATFORD
CV37 1NX

9.2 An acknowledgement will be sent within 5 working days which may request identification verification.

9.3 The request will be complied with within one month of receipt of the request.

10 Complaint

10.1 If the applicant/data subject is dissatisfied with the way in which his/her request has been handled then he/she has the right to make a complaint in accordance with the complaint's procedures of Ettington Parish Council.

In addition, he/she has the right to make a complaint to the Information Commissioner at:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Glossary

Data Controller – The person who (either alone or with others) decides what personal information Ettington Parish Council will hold and how it will be held or used.
Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.
Data Protection Officer – The person(s) responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998
Data Subject/Service User – The individual whose personal information is being held or processed by Ettington Parish Council (for example: a client, an employee, a supporter)
'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject to the processing* of personal information* about her/him. Explicit consent is needed for processing sensitive* data
* See definition
Notification – Notifying the Information Commissioner about the data processing activities of Ettington Parish Council, as certain activities may be exempt from notification.
Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.
Processing – Means collecting, amending, handling, storing or disclosing personal information
Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within Ettington Parish Council.
Sensitive data – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal records
- Criminal proceedings relating to a data subject's offences

Data Controller
Ettington Parish Council is the Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely

to hold, and the general purposes that this data will be used for.

Disclosure

Ettington Parish Council may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Ettington

Parish Council to disclose data (including sensitive data) without the data subject's consent.