Easton Parish Council

Data Protection Policy

Purpose of the policy
This policy explains to councillors, staff and the public about data protection. 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 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
The General Data Protection Regulations and the Data Protection Act 2018 require that everyone within the council must understand the implications of data protection and that roles and duties must be assigned. The Council is the data controller. It is the Clerk'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.

Data protection regulations require 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 is 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.

Data breaches
The Clerk will investigate data breaches. 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 Clerk will also 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 members to use IT in any way that may cause problems for the Council.

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 2018 (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 (if applicable). 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. Where consent is being relied on as the lawful basis for processing the data, privacy notices must be verifiable.

Information Audit
The Clerk 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.

Individuals' Rights
GDPR gives individuals rights:

- 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 incl. profiling.

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

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply.

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 aged 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.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection is included on the Council's Risk Management Policy.

This policy document is written with current information and advice. It will be reviewed regularly 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.

Adopted 3 December 2024