# Carbrooke Parish Council
# General Data Protection Regulation Policy

## Policy Statement

This policy explains to councillors, staff and the public about the General Data Protection Regulation (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 has confirmed that despite the UK leaving the EU, the 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 and the Clerk is the Data Protection Officer (DPO). It is the DPO's duty to undertake an information audit, to manage the information collected by the Council, to issue privacy statements, to deal with requests and complaints raised and deal with the safe disposal of information. This will be included in the job description of the Clerk.

Appointing the Clerk as the DPO must avoid any conflict of interests, in that the DPO should not determine the purpose 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 a high/medium risk to the Council (both financially and in terms of reputation) 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 where necessary and providing a privacy statement on the Council's website, maintaining privacy impact assessments (an audit of potential data protection risks for new projects), minimising who holds data protected information and undertaking training in data protection awareness for the Council.

## 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 Data Protection Working Group. 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 terms of damage to the Council's reputation 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 General Data Protection Regulation. 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 will 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.

**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. 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.

**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.

Individuals have a right to have their personal data erased (sometimes 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 carried out 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.

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 Freedom of Information Publication Scheme. The GDPR Working Group 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, 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 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 will be issued when appropriate

- A privacy statement will be included on the Council's website.

- Data Protection will be included in the Council's Risk Management Policy.

- A Working Group, with terms of reference, will monitor 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 to protect privacy, confidentiality and the interests of the Council.

Agreed: February 2020

Review Date: January 2022 (or sooner if changes in the law require earlier review)