

BONINGALE PARISH COUNCIL

Data Protection Policy

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

This policy explains to councillors, staff and the public the implications of 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. It must be accurate and kept up to date. It must be kept only for as long as is necessary for processing and it must 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 to 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 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/RFO 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 information.

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.

Data Protection requires continued care by everyone within the council, councillors and employees, 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 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 (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

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. Procedures should be in place to detect, investigate and report 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.

Employees, volunteers and members must be careful not to use IT in any way that can be deemed unacceptable conduct, for example, the discussion of internal council matters on social media sites could result in reputational damage for the council and to individuals.

Privacy notices

Being transparent and providing accessible information to individuals about how the councils uses personal data is a key element of the Data Protection Act 1988 (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 where children are involved, although some changes could be needed depending on the situation. All privacy notices must be verifiable.

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 the 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 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 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;
- the 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 (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 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. If a request is perceived to be 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 parish council will be informed of such requests.

Children

There is special provision 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 the age of 13 the council must obtain a parent or guardian's consent in order to process the information 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 must be available on the council's website;
- the clerk's job description must 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 on the council's Risk Management Policy;
- 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.