Brandeston Parish Council GDPR Policy

Purpose of the policy and background to the General Data Protection Regulation
This policy explains to councillors, employees, 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 has been produced to fully incorporate the requirements of the UK Data Protection Act of 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 it identifies how the council will meet its obligations.

Identifying the roles and minimising risk
GDPR requires that everyone within the parish council must understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller and must appoint a Data Protection Officer (DPO). It is the DPO's duty to undertake an information audit and to manage the information collected by the council. A council must adhere to the issuing of privacy statements, dealing with requests and complaints raised and the safe disposal of information.

GDPR requires continued care by everyone within the council 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 to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as a high priority to the council, both reputationally and financially. 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.

The Parish Council has access to the following personal data, stored in a variety of ways:

- Parish Councillors' personal e-mail addresses – normally used for all electronic correspondence between the Councillors and the Parish Clerk.
- Parish Councillors' home addresses and phone numbers, retained by the Parish Clerk.
- Parish Councillors' home addresses, sponsorship, contracts, employment details, licences, corporate tenancies, securities – declared every year on the Register of Councillors Interests, or more recently the Register of Member's Interests form.
- Parish Clerk's name, address and telephone number, and Parish Councillors names only, published on the Brandeston village website
- Parish Clerk's name, address, telephone number and e-mail address published on the ESC website and these details are also accessible via the SCC website which has a link through to Suffolk Infolink via infolink@suffolk.gov.uk, where the Parish Clerk's full details are also published.

- Parish Clerk's name, telephone number and e-mail address on each PC agenda which is circulated to all Brandeston parishioners by e-mail and to the public via the village website.
- Parish Clerk's salary details and contract of employment held on file. Salary information shared with Payroll Administrator and HMRC and included within Annual Accounts that are published on the Parish Website.
- All Parishioners' names and address, recorded on the Electoral Roll, a copy of which is retained by the Parish Clerk.
- All letters, from parishioners are held on file by the Parish clerk in a lockable filing cabinet and all emails from parishioners that are held on the Councils laptops, PCs or other devices which have secure passwords.
- Where Councillors receive Emails directly from a data subject, the Councillor will secure their consent before sharing their data any further. Once this has been obtained, the correspondence will be forwarded immediately to the Clerk of Brandeston Parish Council email address and no other recipient. This information will then be shared at the next Parish Council meeting, but the data subject will not be referred to by name.
- Where the Parish Clerk, or any other member of the Parish Council, receives e-mails from ESC, SCC or SALC, this data is already in the public domain and hence deemed to be low risk. However, such data will still be handled and stored securely in line with this policy.
- E-mails received by PC members from village hall committee members is deemed low risk as the committee members names, addresses and phone numbers are currently recorded on the village website and hence already in the public domain. This is acceptable if consent has been obtained in the first place to share their personal information in this way.
- 100 club parishioners name, addresses, e-mail details are visible on the 100+ club membership form visible to the 100-club organiser.
- Any personal data which is printed off for storage or carriage to meetings for discussion, is subject to the following policy:
    - Consent to share this data must have been obtained in the first place prior to circulation.
    - Where it is deemed necessary for documents to be printed off and stored, these must be kept under lock and key by the Parish Clerk.

Data breaches

One of the duties assigned to the Data Protection Officer (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. 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.

Employees, volunteers, and members must be careful not to use personal data 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 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.

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 and recorded 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 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 (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. 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 council 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 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 Brandeston village website. The policy will be considered as a core policy for the Council.
- 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.

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 always comply with this policy to protect privacy, confidentiality, and the interests of the Council.

An annual review of the training received by members of the Parish Council on GDPR will be undertaken at each May parish Council Meeting to ensure the necessary understanding and awareness of responsibilities.

The initial draft was produced by Councillor S Bange (DPO) and reviewed by R summers (Chair of the Brandeston Parish Council) on 5th September 2022.

Agreed and implemented on 12th September 2022

Version number	Purpose/change	Author	Date
0.1	Initial draft	SB	27/08/2022
0.2	Updated version following review by Chair of Brandeston PC	SB	05/09/2022