BARRINTON PARISH COUNCIL
General Data Protection Regulation Policy

Barrington Parish Council recognises its responsibility to comply with the General Data Protection Regulation which became law on 25th May 2018.

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.

Personal Information is any information that may identify a living individual.

When dealing with Personal Information, the Council's officers and Councillors must ensure that:

- **Data is processed fairly and lawfully**
  Personal information should only be collected from individuals if officers and Councillors have been open and honest about why they want the personal information.
- **Data is processed for specified purposes only**
  The information gained must only be held, used and disclosed for the purpose for which it was obtained.
- **Data is relevant to what it is needed for**
  Information will be monitored so that too much or too little is not kept; only information that is needed should be held.
- **Data is accurate and kept up to date**
  Personal Information should be accurate, if it is not it should be corrected.
- **Data is not kept longer than it is needed**
  Information no longer needed will be shredded or securely disposed of.
- **Data is processed in accordance with the rights of individuals**
  Individuals must be informed, upon request, of all the personal information held about them.
- **Data is kept securely**
  Only officers and Councillors can access the information. It cannot be accessed by members of the public.

Storing and accessing data
All personal information is stored in a filing cabinet at the Parish Clerk's office and all information stored on the Council's computers is password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of Council's document retention policy, it must be shredded or securely deleted from the computer.

The Council is aware that people have the right to access any personal information that is held about them. If a person makes a subject access request (SAR) to see any data that is being held about them the Council must be send to them a copy of all of the personal information that is held about them within a calendar month of the request . The requestor must prove that they are the individual about whom the information has been requested, by way of photographic identification.

Disclosure of personal information
A Councillor may have access to Personal Information to help carry out their duties. This access will be limited to information which is necessary for the purpose and the information should only be used for that specific purpose. Information must not be used for political reasons unless the individual has consented. Personal Information can be disclosed to third parties if that disclosure is in accordance with a legal requirement eg for payroll purposes.

Confidentiality
The Council's officers and Councillors must be aware that when complaints or queries are made, these must remain confidential unless the individual gives permission otherwise.

Additional GPDR Requirements
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 Council is the data controller ~~and the Council will need to appoint a Data Protection Officer (DPO) and will be advised on suitable people by CAPALC.~~
- It is the Clerks role 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.
- ~~*The appointment of the DPO must be a competent person and the appointment of the DPO is the responsibility of the Council. – not sure this is still a pc requirement and am seeking clarification.*~~

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 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
Personal data breaches should be reported to the Clerk for investigation. Any investigation will be supported by the Parish 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, they will need to be contacted directly.

It is unacceptable for non-authorised users to access IT using the clerks 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, 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 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 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.

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 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. 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 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.

This policy is written with current information and will be reviewed 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

This policy will be reviewed Annually

Adopted

Review