

BRISTON PARISH COUNCIL

The Parish Office

Recreation Ground, Stone Beck Lane,

Briston, Melton Constable NR24 2PS

Telephone: 01263 862638

Email: parish-council@briston-norfolk.org.uk

Website: <http://bristonparishcouncil.org/1&1>

Briston Parish Council

General Data Protection Regulation Policy

Adopted:

To be reviewed annually/date of next review May 2019

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

This policy explains to councillors, staff 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 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 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 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). (Clerks are data processors working under the 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. This will be included in the Job Description of the clerk.

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.

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 high / 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 Personnel Committee. 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-authorized 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, for example the discussion of internal

Data subjects

The individuals to whom the data relates.

Data portability

This relates to a request for data relating to an individual, i.e. taking data from one piece of software and putting it into another and providing it in the format readable for the recipient.

Personal Data

This comprises copies of both paper and computer records and related information.

Privacy Statement

A notice detailing, among other things, how the data controller intends to use the personal information they have.

Sensitive Personal Data

Includes information about someone's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexuality and criminal proceedings or convictions. Sensitive personal data can only be processed under strict conditions. In most cases, this means getting express permission from the person the information is about.

Subject Access Request

The right to get a copy of the information held about you. Manifestly unfounded requests could be refused or a charge made. The ICO are to advise about charges.

Automated decision making

The right of subject access for information about the reasoning behind any decisions taken by automated means.

The Cloud

This can be likened to a self-storage warehouse which houses files and allows access from anywhere with an internet connection.

Information Commissioner (ICO)

The independent body which oversees the handling of information.

Information Security Incident (ISI)

The process of managing a breach.

Privacy Impact Assessment (PIA)

The Regulation makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs mandatory in certain circumstances. PIAs are part of privacy by design, and they are processes intended to minimise risk.

Department for Digital, Culture, Media and Sport (DCMS)

The Government Department which has the remit for GDPR.

General Data Protection Regulation

Glossary of key terms, words and abbreviations

What is meant by processing?

The definition of processing is very wide and includes:

- obtaining, recording and holding data
- performing any operation on the data, including the erasure or destruction of the data.

What is personal data?

Personal data is information relating to an identified or identifiable living individual. This may come from the data or from the data **and** other information which is in the possession of, or is likely to come into the possession of, the data controller. The information can be in either electronic or manual form.

Electronic data

Personal data is caught by the Act if the information is being processed, or is recorded with the intention that it should be processed, 'by means of equipment operating automatically in response to instructions given for that purpose'. For all practical purposes this means any data held in electronic form.

The Information Commissioner has advised that **email messages** may be caught by the Act if they identify living individuals and are held, in automated form, in live, archive or back-up systems, or have been deleted from the live system but are still capable of recovery. They could also be caught if, despite having been deleted from the electronic system they are stored in paper form, in relevant filing systems (see next paragraph).

Manual data (data recorded on paper only)

In relation to public bodies, data protection covers all recorded personal data whether this is kept in paper or electronic form. Prior to November 2005, paper data had to be kept as part of 'a relevant filing system' to be within the scope of the DPA. That is no longer the case.

Data controller

The organisation in control of processing the data. The organisation must be a legal entity. Everyone involved with that organisation whether employed or a councillor and who processes personal data has a duty to discharge the data controller's responsibilities. The data controller determines the purposes for which and the manner in which any personal data is processed and is responsible for ensuring compliance with the Regulations.

Data processor

The person responsible to the data protection officer / controller. This could be an external agency, but the data controller is still responsible.

Data Protection Officer (DPO)

The person responsible for data protection compliance. A council can decide who to appoint as a DPO. It could be the Clerk, but a council should avoid a conflict.

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 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 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 Personnel Committee 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 policy will be considered as a core policy for the Council.
- 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 must be issued.
- Data Protection will be included on the Council's Risk Management Policy.
- A Committee, with Terms of Reference, will be set up to 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.

This Policy is supported by the Terms of Reference for the Data Protection Committee (attached).

Signed:

N. Fyfe

*re-adopted 1st April
N. Fyfe*

Dated:

3 September 2018