BERRYNARBOR PARISH COUNCIL

Data Protection Policy

Contents

Introduction

Berrynarbor Parish Council supports the objectives of the Data Protection Act 2018 (the DPA) and intends to conform to the requirements of the Act, and any other applicable legislation at all times.

This Policy must be complied with fully by all Elected Members, Staff, Agents Partners and Contractors of Berrynarbor Parish Council who collect, hold, process or deal with Personal Data for or on behalf of Berrynarbor Parish Council.

In order to operate efficiently Berrynarbor Parish Council needs to collect and use information about people. These may include members of the public, current, past and prospective employees, service users and suppliers. Furthermore, the Council may be required by law to collect and use certain types of information to comply with the requirements of the Government organisations.

All personal information must be handled and dealt with in accordance with the Act, whether the information is collected in paper, electronic or other means.

Processing Personal Data

Personal Data must be processed fairly and lawfully in accordance with the Provisions of the DPA. Personal Data may only be processed for notified purposes as stated with the DPA.

Anyone with responsibility for holding or collecting data must ensure that data kept and processed about any Data Subject is accurate and up to date and kept securely. All due skill and care must be taken. Data must not be excessive to need and superfluous data must be destroyed or removed from the system.

Data shall be processed in accordance with the rights of data subjects under the Act.

Data shall not be transferred to a country or territory outside the European Economics Area, unless that country or territory ensures an adequate level of data protection.

Berrynarbor Parish Council is not a public authority for the purposes of GDPR[1] and therefore does not need to appoint a Data Protection Officer. It will however appoint a Data Protection Lead to ensure due processes are followed.

Berrynarbor Parish Council is responsible for ensuring compliance with this policy and nominates The Data Protection Lead and Clerk to ensure compliance with the Act and ensure that members of staff are aware of the provisions of the Act. The nomination of such a persons shall not release other members of the Council from compliance with this Act and this Policy.

Any processing of sensitive data must comply with the special and more stringent rules set out in the DPA.

Security and Registration

Each Member, member of staff and Data Holder is responsible for ensuring that data cannot be accessed by unauthorised personnel and to ensure that data cannot be tampered with, lost or damaged. All superfluous data must be disposed of in a secure manner.

The Information Commissioner enforces and oversees the DPA and the Freedom of Information Act 2000[2] (FOI). The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. The Information Commissioner keeps a register of all organisations, which process data.

The Council shall submit a Notification to the Information Commissioner and pay the requisite fee at least once a year, which will be dealt with by The Clerk. Members and staff of Council must furnish The Clerk with any information requested for this purpose. Members and staff of Council must notify The Clerk if, during the course of any year, this information changes, and The Clerk must update the Register entry accordingly. Members may have to register personally with the Information Commissioner with respect to constituency or party records.

Agents, Partner Organisations and Contractors

If a Contractor, Partner Organisation or Agent of Council is appointed or engaged to collect, hold, process or deal with Personal Data for or on behalf of Council or if they will do so as part of the services they are providing to Council, The Clerk must as part of evaluation obtain confirmation that the Agent, Partner Organisation or Contractor is able, willing and does comply with the DPA. There must be specific

[1] Data Protection Act 2018, Section 7 (3)
[2] Freedom of Information Act 2000

obligations in every such partnership agreement *and* contract requiring the Partner/Contractor to comply with the DPA.

Disclosure of Personal Data

Personal Data will only be disclosed in accordance with the provisions of the DPA.

Access Rights by Individuals

An individual may request a copy of any data held about them, or information about the reason it is kept and processed and the people to whom it is disclosed. The information must be provided, in clearly understandable terms within 40 days of a valid written request and the payment of the required fee.

A person seeking information shall be required to prove their identity in accordance with the DPA. The 40 days will run from the date the date the person provides this information, and pays any required fee.

Information may be withheld where Council is not satisfied that the person requesting information about themselves are who they say they are, or when the requester is an organisation or body holding itself out as requesting information on behalf of a named individual and the Council is not satisfied that they have the authority to receive that information.

Disclosure to and About Third Parties

Personal Data must not be disclosed about a Third Party except in accordance with the DPA. If it appears absolutely necessary to disclose information about a Third Party to a person requesting data about themselves advice must be sought from The Clerk.

Inaccurate Data

If an individual complains that the data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy.

An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

Requests by Individuals to Stop Processing Information

If data is properly held for marketing purposes, an individual is entitled to require that this is ceased as soon as possible. Requests must be made in writing but generally

all written or oral requests should be heeded as soon as they are made. The cessation must be confirmed in writing.

If data is held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data is held in connection with a contract with the person, if the Council is fulfilling a legal requirement or if the person's vital interests are being protected. Valid written requests must be heeded within 21 days. The cessation must be confirmed in writing.

Complaints

Any complaint or concern expressed by an individual in connection with the DPA must be reported to The Clerk immediately in case legal action is taken. The Clerk will ensure that there has been no breach of the DPA and, if there has, what action needs to be taken to remedy the situation.

Exemptions

There are a number of purposes, which are exempt from certain provisions of the DPA. These purposes are listed in Clause 13 of the Data Protection Guidance. If you are in doubt about which purposes are exempt and the scope of the exemption please contact The Clerk.

Violations of Rules and Procedures

It is the responsibility of all members of staff to report any suspected breaches of the DPA, or of this Policy, to The Clerk.

It is the responsibility of all Members to report any suspected breaches of the DPA, or this Policy, to The Clerk.

Failure to comply with this Policy by employees of Council may result in disciplinary action being taken. Failure to comply by Members of Council may constitute a breach of The Members' Code of Conduct. Failure to comply by partners, agents or contractors may constitute a breach of their agreement.

The policy should be reviewed annually.

Adopted

Date of Review	Change Description	Minute No.
20 March 2026	Data Protection Act updated	2603/14
12 May 2026	Data Protection Lead Role added	2605/07