Boyatt Wood Parish Council

General Data Protection Regulation Policy

Table of Contents

Version Control

Version	Date approved	Minute Ref	Website updated	Next Review
V1	13/06/2023	041/23	10/07/2023	Q2 2025

1. Introduction

The Data Protection Act 2018 (DPA 2018) came into force in the United Kingdom (UK) on 25 May 2018. The DPA 2018 is the UK's implementation of the General Data Protection Regulation (GDPR), and it seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data. It provides a statutory framework for the use of information held about identifiable individuals in the UK.

The UK GDPR and DPA 2018 applies to both automated personal data and manual filing systems.

2. Key principles

The UK GDPR sets out seven key principles, compliance with the spirit of the principles is essential in supporting good data protection practice. Failure to comply with the principles may place the organisation at risk of an administrative fine as described in Article 83 (5) GDPR. The Information Commissioners Office (ICO) can penalise the council for the breach itself and award compensation to the individual(s) adversely affected.

Article 5(1) requires that personal data held shall be subject to

- Lawfulness, fairness and transparency - Processed lawfully
- Purpose limitation – Specified and explicit purpose only
- Data minimisation – Adequate, relevant and limited to what is necessary
- Accurate – Where necessary kept up to date
- Storage limitation – Kept in a form which permits identification and no longer than is necessary
- Integrity and confidentiality (security) – Protects against unauthorised, unlawful processing and against accidental loss, destruction or damage
- Accountability – Able to demonstrate compliance with principles.

3. Controllers and processors

Controllers are the main decision makers and exercise overall control over the purposes and means of the processing of personal data.
Controllers must comply with the data protection principles and UK GDPR requirements and other legislation such as the Human Rights Act and have a legitimate reason for processing personal data. Controllers are also responsible for their processors.
Controllers must pay the data protection fee to the Information Commissioners Office unless exempt.

Processors act on behalf of, and only on the instructions of, the relevant controller. They do not have the same obligation as Controllers, however they do have direct obligations under UK GDPR.

The Council as a corporate body is responsible for ensuring compliance with the legislation, the Council has delegated the day to day responsibility to the Parish Clerk.

4. Processing Information

Boyatt Wood Parish Council (BWPC) is a Data Controller and is registered with the Information Commissioners Office Registration reference ZB483050 and processes personal data in accordance with UK GDPR to

- Fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- Pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- Monitor its activities including the equality and diversity of its activities.
- Assist regulatory and law enforcement agencies.
- Process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- Process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- Undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- Undertake research, audit and quality improvement work to fulfil its objects and purposes.
- Carry out Council administration.
- Process information with the consent of the data subject

Where appropriate and governed by necessary safeguards BWPC will carry out the above processing jointly with other appropriate bodies from time to time.

5. Privacy Notices

Providing accessible information to individuals about the use of their personal information is a key element of their legal right to transparency as set out in the UK GDPR. The Data Controller is responsible for providing this information in an easily accessible format to individuals regarding the manner that BWPC processes their information.
This information is provided in the form of a privacy notice, this is a document that sets out the policies in plain simple language, it identifies the data controller and contact details. It describes BWPC data processing practices and explains the purposes for which personal data is collected, used, and disclosed, how long it is kept, and the controller's legal basis for processing.

6. Rights of Data subjects

UK GDPR gives individuals rights regarding information held on them.

- 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 information provided to individuals must be concise, transparent, intelligible and easily accessible.
If a request is received to rectification, erase (right to be forgotten), restrict processing or object BWPC must respond within one month.

7. Children

Although the legal age of consent under UK GDPR is 13 years or over, BWPC will not hold information relating to a child under the age of 16 years old unless parental/guardian consent has been received in writing.
Children have the same rights as adults over personal data.

8. Minimising Risk

UK GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned.

The Council will endeavour to protect all its data from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure.
Handling of personal information in any form is seen as high / medium risk to the council due to the potential adverse impact both financial and reputational. The risk is minimised through technical measures, training and appropriate policies. BWPC will implement procedures and manage responsibly, all data it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

The Council will be as transparent as possible about its operations and will work closely with public, community, key stakeholders, and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the community. Details of information which is routinely available is contained in the BWPC's Publication Scheme.

9. Data Breaches

The Data controller must report a personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach. If the data breach is likely to result in a risk to rights and freedoms of peoples it must be reported without delay
As soon as the Data Controller is aware of the breach there are immediate actions that should be taken and an investigation commenced.

I. Commence a log

Immediately commence a log of the full details of the breach. To include who reported the breach and how it was identified.

II. Find out what happened

Pull the facts together quickly as possible, maintain the timeline in the log – Liaise with ICO

III. Contain Breach

The priority is to establish what has happened to the personal data. If the data can be recovered do so immediately.
Protect those that will be impacted by the breach. Provide advice if necessary and assist where able.

IV. Assess the risk

Review the situation in detail and assess harm (if any) caused to those affected. Review procedures and update/amend as required to prevent further breaches.

V. Report

If the breach is reportable to ICO, submit report.

10. Definitions

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis

Personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction