BRACEBRIDGE HEATH PARISH COUNCIL

Bracebridge Heath Community Library, London Road, Bracebridge Heath, Lincoln, LN4 2LA
07899 888530 – clerk@bracebridgeheath-pc.gov.uk

Data Protection Policy

Contents **Page**

1. Purpose 1

2. Scope 1

3. Policy Statement 1

4. Definitions 1

5. Responsibilities & review 2

6. Related legislation, policies and guidance 2

7. Procedure

   7.1. Storing data 2
   7.2. Accessing data 3

8. Data breaches

   8.1. Consequences of a personal data breach 3
   8.2. Duty to report a breach 3
   8.3. Data processors duty to inform the Parish Council 4
   8.4. Records of data breaches 4

9. Version control and amendment history 4

10. Appendices 5

    Appendix 1 – Security compliance checklist 5

    Appendix 2 – Consent form for electronic communications 6

1 Purpose

1.1 The purpose of this policy is to ensure that employees, councillors and volunteers handing personal information at Bracebridge Heath Parish Council (the 'Parish Council') are fully aware of the requirements of the General Data Protection Regulations (GDPR) and comply with data protection procedures. The policy also aims to ensure that data subjects are aware of their rights.

1.2 The aim of this policy is to outline how the Parish Council meets its legal obligations in safeguarding confidentiality and adheres to information security standards.

2 Scope

2.1 This policy applies to all councillors, employees and volunteers of Bracebridge Heath Parish Council and will be referred to as role holders within this policy.

2.2 This Data Protection Policy covers;

- the processing of all personal information whose use is controlled by the Parish Council;
- all personal information handled, stored, processed or shared by the Parish Council whether organised and stored in physical or IT based record systems.

3 Policy statement

3.1 The Parish Council recognises its responsibility to comply with the GDPR 2018 which regulates the use of personal data.

3.2 Role holders have a duty to comply with the policy when handling personal data.

4 Definitions

4.1 A list of definitions of the technical terms used in this policy is below:

- Data Controller
  The person(s) who, on behalf of the Parish Council, decides what personal information the Parish Council will hold and how long it will be held or used

- Data Protection Officer
  The person(s) responsible for ensuring that the Parish Council follows data protection policy and complies with the relevant legislation.

- Information Commissioner's Office (ICO)
  A UK independent body responsible for upholding the information rights of the public.

- Personal Information
  Information about living individuals that enables them to be identified. E.g. names and addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers, employees or members of the public.

- Sensitive data
  Includes but is not limited to data relating to racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, criminal record or proceedings.

5 Responsibilities & review

5.1 All role holders are responsible for the safeguarding of personal data they come into contact with whilst carrying out duties on behalf of the Parish Council.

5.2 All role holders are responsible for maintaining confidentiality of complaints or queries made by members of the public unless the subject has given permission otherwise.

5.3 The Full Council is responsible for the review of this policy on a biennial basis or in response to changes in relevant legislation.

6 Related legislation, policies & guidance

6.1 This policy is not a substitute for legislation, regulations and codes of practice but defines how the Council will apply the relevant legislation. Related legislation, policies and guidance is listed below:

- Data Protection Act 2018
- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- General Data Protection Regulations (GDPR) 2018
  The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protections principles. GDPR recitals add depth and help to explain the binding articles. Recitals are not legally binding but are useful for understanding the articles.

Bracebridge Heath Parish Council internal documents:

- Subject Access Request Procedure
- Privacy notices
- Document Retention Policy
- Freedom of Information policy

7 Procedure

7.1 Storing data

7.1.1 The Parish Council recognises its responsibility to be open with people when taking personal details from them. This means that employees must be honest about why they want a particular piece of personal information.

7.1.2 The Parish Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept within Parish Council facilities and are not available for public access. All data stored by the Parish Council is secured with password protection on office computers.

7.1.3 When data is no longer needed, is out of date or has served its use and falls outside of the minimum retention period specified within the Parish Council's

Document Retention Policy it will be shredded or securely deleted from the computer.

7.2 **Accessing data**

7.2.1 The Parish Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy or email).

7.2.2 Full details of Subject Access Requests can be found in the Subject Access Request procedure adopted by the Parish Council.

8 Data breaches

8.1 GDPR defines a personal data breach as a 'breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processes'. Examples include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration pf personal data without permission;
- loss of availability of personal data.

8.2 The Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets

8.3 **Consequences of a personal data breach**

8.3.1 A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality or personal data, damage to property or social disadvantage. Therefore, a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

8.4 **Duty to report a breach**

8.4.1 If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and Information Commissioners Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

8.4.2 The Data Protection Officer must be informed immediately so they are able to report to the ICO in the 72 hours window.

8.4.3 If the ICO is not informed within 72 hours, Bracebridge Heath Paris Council via the DPO must give reasons for the delay when they report the breach.

8.4.4 When notifying the ICO of a breach, Bracebridge Heath Parish Council must:

I. describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
II. communicate the name and contact details of the DPO;
III. describe the likely consequences of the breach;

IV. describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effect.

8.4.5 When notifying the individual affected by the breach, the Parish Council must provide the individual with (ii)-(iv) above.

8.4.6 The Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- it has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- it would involve a disproportionate effort.

However, the ICO must still be informed even if the above measures are in place.

8.4.7 To report a breach, use the ICO online system at https://ico.org.uk/for-organisations/report-a-breach/

8.5 **Data processors duty to inform the Parish Council**

8.5.1 If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify the Parish Council without undue delay. It is then the Parish Council's responsibility to inform the ICO as the data controller.

8.6 **Records of data breaches**

8.6.1 All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify the system failures and should be used as a way to improve the security of personal data.

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO / individual	Actions to prevent breach recurring

9 Version control and amendment history

Date approved	Version Number	Revision / amendments made	Review date
April 2014	1.0	New policy	March 2015
April 2017	1.1	Reviewed – no changes	April 2018
21 May 2018	2.0	Revised in line with GDPR	May 2020
17 June 2020	2.1	Policy review – references to role holders, Finance & Policy committee, updated legislation to UK-GDPR	June 2023
June 2023	2.2	Updated document header Removal of references to committees Removal of Appendix 2 – consent form for contacting members of council. This is no	June 2025

		longer relevant as all member of council are issues a corporate email address.	

Appendix 1 -Security compliance checklist

BRACEBRIDGE HEATH PARISH COUNCIL

Bracebridge Heath Community Library, London Road, Bracebridge Heath, Lincoln, LN4 2LA
07899 888530 – clerk@bracebridgeheath-pc.gov.uk

Security compliance checklist

All employees and councillors should complete the security checklist below to show compliance. Records should be retained whilst they remain in office / post.

	Yes/No
Computer is password protected	
Email is password protected	
Mobile devices are password protected	
Flash drives are password protected	
External hard drives are password protected	
Cloud access is password protected	
Hard copy files are held securely	
Anti-virus software is up to date	
Confirm that council information is kept securely ensuring nobody outside of council has access	

Specify the date compliance will be achieved if you have answered “No” to any of the above:

Date: _____

Employee / Councillor name: _____

Employee / Councillor signature: _____

Date: _____