

BRACEBRIDGE HEATH PARISH COUNCIL

The Heath: Village Hall & Library, Red Hall Lane, Bracebridge Heath, LN4 2LB
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 |
| 7.3. Privacy Notices | 3 |
| 8. Data breaches | |
| 8.1. Data breaches | 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 – Privacy notice – General | 7 |
| Appendix 3 – Privacy notice – Staff, councillors and role holders | 11 |

1 Purpose

- 1.1 The purpose of this policy is to ensure that employees, councillors and volunteers handling 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.
- 1.3 In complying with the Data Protection Act 2018 the Council shall ensure that all data is:
 - a. Processed fairly, lawfully and in a transparent manner
 - b. Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes
 - c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
 - d. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed
 - e. Processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational features

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**
A person appointed by the organisation and is responsible for ensuring that the Parish Council follows data protection policy and complies with the relevant legislation. (Parish Council's are exempt from the requirement to appoint a DPO under Section 7 Data Protection Act)
 - **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 every 3 years 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
 - Privacy and Electronic Communications Regulations
 - 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.
- 7.1.4 The Council will carry out a data audit annually to ensure that data is held and stored appropriately. A data map outlining the storage locations for personal information held by the council will be updated annually.

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.

7.3 Privacy notices

- 7.3.1 Privacy notices will be prepared and reviewed by the council at least every 3 years in line with the scheduled policy review.
- 7.3.2 Privacy information will be provided to individuals at the point of collection. This may be done by referring individuals to the council's website where the privacy notice is published.

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 of personal data without permission;
 - loss of availability of personal data.

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

8.2 Duty to report a breach

- 8.2.1 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.
- 8.2.2 If the ICO is not informed within 72 hours, Bracebridge Heath Parish Council must give reasons for the delay when they report the breach.

8.2.3 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 (if they have one);
- 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.

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

8.2.5 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.

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

8.3 Data processors duty to inform the Parish Council

8.3.1 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.

8.4 Records of data breaches

8.4.1 All data breaches must be recorded internally and reported to the full council 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 longer relevant as all member of council are issued a corporate email address. | June 2025 |
| June 2025 | 2.3 | <ul style="list-style-type: none"> - Updated document header - Removal of reference to Data Protection Officer (DPO). Parish Councils are exempt from the requirement to appoint a - DPO under s7 DPA 2018) - Scheduled review period changed from every 2 years to every 3 years. - Included additional information about privacy notices and appended the notices to the policy. - Included details of the principles of the DPA. | June 2028 |

Appendix 1 -Security compliance checklist

BRACEBRIDGE HEATH PARISH COUNCIL

The Heath: Village Hall & Library, Red Hall Lane, Bracebridge Heath, LN4 2LB
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 |
|---|--------|
| Computers/devices are 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 | |
| I 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: _____

Appendix 2 - GENERAL PRIVACY NOTICE

Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the “GDPR”) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Bracebridge Heath Parish Council which is the data controller for your data.

Other data controllers the council works with:

- Other local authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Credit reference agencies

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be “joint data controllers” which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The Council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
 - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
 - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
 - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as “Special categories of data” and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
 - In limited circumstances, with your explicit written consent.
 - Where we need to carry out our legal obligations.
 - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about;
- kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.
- Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy

Sometimes the use of your personal data requires your consent. We will first obtain your consent for that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data. When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) *The right to access personal data we hold on you*

At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.

There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) *The right to correct and update the personal data we hold on you*

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) *The right to have your personal data erased*

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.

When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) *The right to object to processing of your personal data or to restrict it to certain purposes only*

You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) *The right to data portability*

You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*

You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) *The right to lodge a complaint with the Information Commissioner's Office.*

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page <http://parishes.lincolnshire.gov.uk/BracebridgeHeath/index.asp?catId=14011>. This notice was last updated in June 2025.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Bracebridge Heath Parish Council, The Heath: Village Hall & Library, Red Hall Lane, Bracebridge Heath, LN4 2LB

Email: clerk@bracebridgeheath-pc.gov.uk

Appendix 3 - PRIVACY NOTICE

For staff*, councillors and role holders**

**“Staff” means employees, workers, agency staff and those retained on a temporary or permanent basis*

***Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.*

Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the “GDPR”) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Bracebridge Heath Parish Council which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be “joint data controllers”. This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes.
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about;
- kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date.
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.

- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note we need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer councillors' interests
- To provide a reference.
- Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data. We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

How we use sensitive personal data

- We may process sensitive personal data relating to staff, councillors and role holders including, as appropriate:
 - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
 - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
 - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
 - In limited circumstances, with your explicit written consent.
 - Where we need to carry out our legal obligations.
 - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
 - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.] [Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation. We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- other persons or organisations operating within local community.
- other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- staff pension providers
- former and prospective employers
- DBS services suppliers
- payroll services providers
- recruitment Agencies
- credit reference agencies
- professional advisors
- trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. *The right to access personal data we hold on you*

At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.

There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. *The right to correct and update the personal data we hold on you*

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. *The right to have your personal data erased*

If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.

When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. *The right to object to processing of your personal data or to restrict it to certain purposes only*

You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. *The right to data portability*

You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*

You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. *The right to lodge a complaint with the Information Commissioner's Office.*

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page <http://parishes.lincolnshire.gov.uk/BracebridgeHeath/index.asp?catId=14011>. This Notice was last updated in June 2025.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Bracebridge Heath Parish Council, Bracebridge Heath Community Library,
London Road, Bracebridge Heath, LN4 2LA

Email: Clerk@bracebridgeheath-pc.gov.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.