

Billingsborough Parish Council

Data Protection, Publication & Freedom of Information Policies & Procedures

Data Protection Policy

1. Billingsborough Parish Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 which regulates the use of personal data. This does not have to be sensitive data; it can be as little as a name and address.

General Data Protection Regulations (GDPR)

2. The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used. The GDPR applies to anyone holding personal information about people, electronically or on paper. The Council has also registered with and notified the Information Commissioner that it holds personal data about individuals.
3. When dealing with personal data, Council staff and members must ensure that:
 - **Data is processed fairly, lawfully and in a transparent manner**
This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.
 - **Data is processed for specified purposes only**
This means that data is collected for specific, explicit and legitimate purposes only.
 - **Data is relevant to what it is needed for**
Data will be monitored so that too much or too little is not kept; only data that is needed should be held.
 - **Data is accurate and kept up to date and is not kept longer than it is needed**
Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.
 - **Data is processed in accordance with the rights of individuals**
Individuals must be informed, upon request, of all the personal information held about them.
 - **Data is kept securely**
There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data Controller.

4. Billingborough Parish Council is the Data Controller, which means that it is the Council that determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

Data Collection.

5. Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.
6. Billingborough Parish Council will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form. When collecting data, the Council will ensure that the Data Subject:
 - Clearly understands why the information is needed
 - Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent
 - As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
 - Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
 - Has received sufficient information on why their data is needed and how it will be used

Storing & Accessing Data

7. Billingborough Parish Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.
8. The Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the registered address of the Council and are not available for public access. All data stored on the Council computer is password protected. Once data is not needed any more, is out of date or has served its use and falls outside the minimum retention time of Councils document retention policy, it will be shredded or securely deleted from the computer.
9. The 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, email or social media).

If a person requests to see any data that is being held about them, the SAR response must detail:

- How and to what purpose personal data is processed
- The period the Council tend to process it for
- Anyone who has access to the personal data

10. The response must be sent within 30 days and should be free of charge.
11. If a SAR includes personal data of other individuals, the Council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.
12. Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests. Refer to the SAR Procedure at **Annex A** for more details.

Confidentiality.

13. Billingborough Parish Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential.

Records Retention Policy

1. Billingborough Parish Council recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the association. This document provides the policy framework through which this effective management can be achieved and audited. It covers:
 - Scope
 - Responsibilities
 - Retention Schedule

Scope

2. The Records Retention Policy applies to all records created, received or maintained by Billingborough Parish Council in the course of carrying out its functions.

3. Records are defined as all those documents which facilitate the business carried out by Billingborough Parish Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically. A small percentage of Billingborough Parish Council records may be selected for permanent preservation as part of the Councils archives and for historical research.

Responsibilities

4. Billingborough Parish Council has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Clerk.
5. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely. Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with Billingborough Parish Council's records management guidelines.

Retention Schedule

6. The retention schedule detailed at **Annex B** refers to records retained by Billingborough Parish Council and the reason why, regardless of the media in which they are stored.

Data Breach Policy

1. GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". 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
2. Billingborough Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a Personal Data Breach

3. 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 of 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.

Duty to Report a Breach

4. 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 ICO by the Council without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72-hour timeframe.
5. If the ICO is not informed within 72 hours, the Council via the DPO must give reasons for the delay when they report the breach. When notifying the ICO of a breach, the Council must:
 - 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
 - Communicate the name and contact details of the DPO
 - Describe the likely consequences of the breach
 - Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.
6. Data breaches can be reported to the ICO using the online system: <https://ico.org.uk/for-organisations/report-a-breach/>
7. When notifying the individual affected by the breach, the Council must provide the individual with the information at Para 5 above.
8. The 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
9. However, the ICO must still be informed even if the above measures are in place.

Data Processors Duty to Inform

10. If a data processor (i.e. payroll provider or Parish Clerk) becomes aware of a personal data breach, it must notify the Council without undue delay. It is then the Council's responsibility to inform the ICO, not the data processor.

Records of Data Breaches

11. All data breaches must be recorded whether or not they are reported to individuals. The record template at **Annex C** should be completed to identify and record system failures and should be used as a way to improve the security of personal data.

Freedom of Information & Data Publication Scheme

1 Compliance with the Freedom of Information Act 2000 (FOIA) is the legal responsibility of local authorities and other public organisations. It is part of a wider group of national policies which aim to modernise government and show people how it is working on their behalf. Since January 2005 people have had a right to know what decisions are taken on their behalf, and how services are run. They can ask to see not only printed leaflets and other publications, but also any background files and other records relating to the business of the organisation, unless statutory exemptions apply.

2 Section 19 of the FOIA requires every public authority to adopt and maintain a publication scheme, and to publish data in accordance with the scheme. The Council Data Publication Scheme is detailed at **Annex D**. The Scheme makes it clear what information can already be accessed and where it is available. The Publication Scheme outlines any charges that may be made in supplying any information. Any additional information, which is not part of the Publication Scheme, can be requested under the FOIA or SAR.

3 Billingborough Parish Council is on the Information Commissioner's Office (ICO) Register of data controllers. This Register outlines what information is held and processed by the Council, and how it is used.

4 Responsibility for dealing with all requests for information has been delegated to the Clerk to the Council. A request for information must be made in writing by letter or e-mail and should be sent to the Clerk. The request must include a contact name, an address for correspondence and state clearly what information is required and the reason for the request.

5 The first step will be to identify whether the council holds the requested data. If not, the applicant will be notified accordingly. If the information is held, and is not subject to any exemption, it will normally be supplied within 20 working days unless there is a fee to pay, or further clarification must be sought. If the request for information is unclear, the Clerk will contact the applicant to clarify what data is being sought. If clarification of a request is needed, the 20-working day period will commence on receipt of the additional information.

6 If the information is not held by the Council, but the Council is aware of another public body which may hold the information, the request will either be forwarded to the third party concerned, or the applicant will be given details of which public authority is believed to hold the information.

7 Where information cannot be provided, a refusal notice will be issued explaining which exemption applies, and advising of any right to appeal, if applicable.

8 Where information is subject to a 'qualified exemption' under the FOIA, there may be an extension to the 20-working day period whilst further consideration is given to applying the public interest test, to determine whether any information should be withheld or disclosed.

9 Where any complaint is received about the processing of any request for information, this will be referred on to full Council for attention.

10 Where any correspondence is received from the Information Commissioner's Office in relation to any Freedom of Information matter, this will be referred on to full Council for attention.

In case of any queries or questions in relation to Billingborough Parish Council's Data Protection, Publication & Freedom of Information Policies and Procedures, please contact the Parish Clerk as Proper Officer of the Council.

Data Protection, Publication & FOI Policies & Procedures Annexes:

Annex A: SAR Procedure

Annex B: Retention Schedule

Annex C: Data Breach Record

Annex D: Data Publication Scheme

The revised Data Protection, Publication & Freedom of Information Policies and Procedures were adopted by Billingborough Parish Council at its General Meeting on 3 March 2018 and reviewed 10 March 2026.