

Bathampton Parish Council - Data Protection Policy

The Data Protection Policy

Bathampton 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)

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. Bathampton Parish Council has also notified the Information Commissioner that it holds personal data about individuals.

When dealing with personal data, Bathampton Parish 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.

Storing and accessing data

Bathampton 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.

Bathampton Parish Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the Bathampton Parish Council Office and are not available for public access. All data stored on the Bathampton Parish Council Office computers are password protected and must meet the following criteria:

- All passwords must have at least eight characters

- Passwords must contain characters from at least two of the three following groups: Upper- and lower-case alphabetic characters, Numeric characters and Special characters (e.g. ! £ \$. , ? /)
- Passwords created must not be used for other applications such as those used for employee's personal accounts at home. This is to prevent unauthorised persons from easily accessing both.
- All passwords should be reasonably difficult for unauthorised people to guess. Employees should use common sense when choosing their passwords and avoid basic combinations and/or dictionary words that are easy to crack. For instance, choices like 'password', 'password1!' or 'P4\$\$w0rd!' are equally bad from a security perspective.
- Employees should avoid choosing passwords that are based on information that is easily discoverable, such as: pet's name, family members name, Date of birth.
- Default passwords, such as those created for new employees when they start, must be changed by user on the first use.
- New passwords for employees granting access to applications and devices must be authorised by the IT Support Administrator.
- Further information on selecting a strong password can be found here (<https://www.ncsc.gov.uk/cyberaware/home>)
- Employees must never share their passwords with anyone else in the Organisation and must refrain from writing them down. Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

All Pc's must have antivirus software installed to detect and remove any virus automatically. Employees must use only software that is authorised by Bathampton Parish Council on Bathampton Parish Council approved computers. Authorised software must be used in accordance with the software supplier's licensing agreements.

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.

Care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Bathampton Parish Council authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Bathampton 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, 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 Bathampton Parish Council tend to process it for
- Anyone who has access to the personal data.

The response must be sent within 30 days and should be free of charge.

If a SAR includes personal data of other individuals, Bathampton Parish 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.

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.
Please see "Subject Access Request Procedure" for more details.

Confidentiality

Bathampton 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.

Approved and adopted by Bathampton Parish Council: 16th November 2023, Minute Ref:2023/155
Date for review: October 2024