Binsted Parish Council

Data Protection Policy

INTRODUCTION - Binsted Parish Council needs to gather and use certain information about individuals. These can include parishioners, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Parish Council's data protection standards – and to comply with the law.

WHY THIS POLICY EXISTS - This data protection policy ensures that Binsted Parish Council:

- Complies with data protection law and follows good practice
- Protects the rights of staff, parishioners and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW - The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways

POLICY SCOPE - This policy applies to Binsted Parish Council and;

- All staff, councillors and volunteers of Binsted Parish Council
- All contractors, suppliers and other people working on behalf of Binsted Parish Council

It applies to all data that the Council holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include; Names of individuals, postal addresses, email addresses, Telephone numbers and any other information relating to individuals.

DATA PROTECTION RISKS - This policy helps to protect Binsted Parish Council from some very real data security risks, including:

- Breaches of confidentiality: for instance, information being given out inappropriately
- Failing to offer choice; all individuals should be free to choose how the Council uses data relating to them
- Reputational damage: for instance, the Council could suffer if hackers successfully gained access to sensitive data

RESPONSIBILITIES - Everyone who works with or for Binsted Parish Council has some responsibility for ensuring data is collected, stored and handled appropriately.

- Councillors are ultimately responsible for ensuring that Binsted Parish Council meets its legal obligations
- The Data Protection Officer (to be appointed) is responsible for:

i. Keeping councillors updated about data protection responsibilities, risks and issues
ii. Reviewing all data protection procedures and policies, in line with an agreed schedule
iii. Arranging data protection training and advice for the people covered by this policy
iv. Handling data protection questions from anyone covered by this policy
v. Dealing with requests from individuals to see the data Binsted Parish Council holds about them
vi. Checking and approving any contracts or agreements with third parties that may handle the Parish Council's sensitive data.

The Clerk is responsible for:

i. Ensuring all systems, services and equipment used for storing data meet acceptable security standards
ii. Performing regular checks and scans to ensure security hardware and software is functioning properly
iii. Evaluating any third-party services the Parish Council is considering using to store or process data. For instance, cloud computing services.

General Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally
- Binsted Parish Council will ensure that its employees have access to training to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords should be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the Council or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of

Data and Paper Storage - These rules describe how and where data should be safety stored. When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed.

- The paper or files should be kept in a locked office, drawer or filing cabinet
- Employees should ensure paper and printouts are not left where unauthorised people could see them
- Data printouts should be shredded and disposed of securely when no longer required

Electronic Storage - When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared
- If data is stored on removable media these should be kept locked away securely when not used
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service
- Data should be backed up frequently and these backups should be tested regularly
- Data should never be saved directly to laptops or other mobile devices; tablets and smartphones.
- All servers and computers containing data should be protected by approved security software and a firewall

Data Use - When working with personal data, employees should ensure that the screens of their computers are locked when left unattended. Personal data should not be shared informally. In particular, it should never be sent by email. Data must be encrypted before being transferred electronically.

Data Accuracy - The law requires Binsted Parish Council to take reasonable steps to ensure data is kept accurate and up to date.

- Data will be kept in as few places as necessary
- Every opportunity should be taken to ensure data is updated
- Binsted Parish Council will make it easy for data subjects to updated regularly on the Parish Council website
- Data should be updated as inaccuracies are discovered.

Subject Access Requests - All individuals who are the subject of personal data held by Binsted Parish Council are entitled to:

- Ask what information the council holds about them and why
- Ask how to gain access to it
- Be informed about how to keep it up to date
- Be informed how the council is meeting its data protection obligations

A request from an individual for this information is a Subject Access Request. Subject access requests should be made by email, addressed to the data controller, the data controller will ensure the request is legitimate.

Providing information - Binsted Parish Council aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, Binsted Parish Council has a privacy statement setting out how data relating to individuals is used the authority. This is available on request and is also available on the Parish Council's website.

Adopted: 1st November 2021
Review due: November 2022