INFORMATION AND DATA PROTECTION POLICY

FEBRUARY 2023

Adopted: 23 February 2023
Review Date: 23 February 2026

BIGGLESWADE TOWN COUNCIL
INFORMATION AND DATA PROTECTION POLICY

Biggleswade Town Council recognises it must, at times, keep and process sensitive and personal information about both employees and the public. It has therefore adopted this policy not only to meet its legal obligations but also to ensure high standards.

The Town Council will be very transparent about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is routinely available is contained in the Town Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Making Information Available

The Publication Scheme is a means by which the Town Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Town Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Town Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Town Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the Website and sent to the local media. The Town Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Town Council welcomes public participation and has a public participation session on each Council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its Website or at its Offices.

Occasionally, the Town Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by the Town Council but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of a Town Council meeting. In other words, decisions which would have been made by the Town Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of Town Council and committee meetings normally open to the public. The Town Council will, where possible, facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without

undermining the broader purpose of the meeting.

The Town Council will be pleased to make special arrangements on request for persons with hearing or sight difficulties.

Protecting Confidential or Sensitive Information

The Data Protection Act 2018 seeks to strike a balance between the rights of individuals and the sometimes-competing interests of those with legitimate reasons for using personal information. The policy is based on these principles:

The Town Council will make any notification required to the Information Commissioner's Office under the Data Protection Act 2018 and periodically update the information.

The Town Council will comply with the eight principles of good practice for processing sensitive data, by ensuring it is:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept longer than is necessary.
- Processed in accordance with the individual's rights.
- Secure.
- Not transferred to countries outside the EU unless the country has adequate protection for the individual.

The Town Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing.
- Processing is necessary for the performance of a contract with the individual.
- Processing is required under a legal obligation.
- Processing is necessary to protect the vital interests of the individual.
- Processing is necessary to carry out public functions.
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any sensitive personal information and The Town Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual.
- Required by law to process the data for employment purposes.
- A requirement in order to protect the vital interests of the individual or another person.

The Town Council will always give guidance on personnel data to employees through the Employee Handbook.

The Town Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Disclosure Information

The Town Council will, as necessary, undertake checks on both staff and Members with the

Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Procedures

The Town Council has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- It appoints or employs employees with specific responsibilities for:
  - the processing and controlling of data;
  - the comprehensive reviewing and auditing of its data protection systems and procedures;
  - overviewing the effectiveness and integrity of all the data that must be protected.

  There are clear lines of responsibility and accountability for these different roles.
- It provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
- It provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.
- It can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.
- It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Town Council.
- It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Town Council understands that consent must be freely given, specific, informed and unambiguous. The Town Council will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- It has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report
- Significant breaches that cause significant harm to the affected individuals to the Information Commissioner and is aware of the possible consequences.
- It is aware of the implications international transfer of personal data internationally.

Access to Information

Relevant individuals have a right to be informed whether the Town Council processes personal data relating to them and to access the data that the Town Council holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- A form on which to make a subject access request ("SAR") is available from the Administration & HR Manager.
- The Town Council will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.
- The Town Council will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the Town Council immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Town Council will take immediate steps to rectify the information.

Data Security

The Town Council adopts procedures designed to maintain the security of data when it is stored and transported. Employees must:

- Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
- Refrain from sending emails containing sensitive work-related information to their personal email address.
- Check regularly on the accuracy of data being entered into computers.
- Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- Use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by a senior manager. Where personal data is recorded on any such device it should be protected by:

- Ensuring that data is recorded on such devices only where absolutely necessary.
- Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
- Ensuring that laptops or USB drives are not left lying around where they can be stolen.
- Ensuring that data access is limited only to staff that need access to the relevant information.

Data Transparency

The Town Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

“Public data” means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council’s decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:

Demand led: new technologies and publication of data should support transparency and accountability.

Open: the provision of public data will be integral to the Council’s engagement with residents so that it drives accountability to them.

Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with a turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Biggleswade Town Council exceeds this turnover but will nevertheless ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts.
- Annual Governance Statements.
- Internal Audit Reports.
- List of Town Councillor or Member responsibilities.
- Details of public land and building assets.
- Draft Minutes of Town Council and committee meetings within one month.
- Agendas and associated papers no later than three clear days before the meeting.