

Banham Parish Council - Data Protection Policy

This policy sets out how the Council manages and protects personal data, and explains data protection requirements to councillors, staff and members of the public. The Council is committed to ensuring that personal data is handled in accordance with applicable data protection legislation. Personal data must be:

- Processed lawfully, fairly, and in a transparent manner
- Collected for specified and legitimate purposes and not further processed in a manner incompatible with those purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Retained only for as long as is necessary for the purposes for which it is processed
- Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

This policy outlines the duties and responsibilities of the Council in relation to data protection and identifies the measures and controls in place to ensure compliance with its obligations.

Identifying the roles and minimising risk

Data protection legislation requires that all individuals within the council understand their responsibilities and the implications of handling personal data. This includes Councillors, employees, and any other persons acting on behalf of the Council. The Clerk to the Council has day to day responsibility for data protection compliance including:

- Undertaking and maintaining an information audit
- Managing the information collected, stored and processed by the Councillors
- Preparing and issuing appropriate privacy statements and notices
- Handling data protection requests and managing any requests and complaints received
- Ensuring the secure storage and safe disposal of personal data

All councillors and staff share responsibility for data protection legislation. This applies to all forms of information, whether held in hard copy or electronically. Particular care must be taken when sharing personal data to ensure that it is only disclosed where necessary. Failure to comply with the regulations could result in the Council facing a fine from the Information Commissioners office as well as potential liability to compensate individuals who may be adversely affected by the breach. The Council seeks to minimise risks associated with data protection through:

- Regular information audits
- Clear and accessible privacy statements
- Limiting access to personal data to those who require it
- Providing appropriate data protection

In addition, the Council has agreed that any personal data circulated to councillors prior to a meeting will be deleted immediately following the meeting. This measure is intended to reduce the risk associated with the unnecessary retention and duplication of personal data.

Data breaches

The Clerk shall be responsible for investigating all reported data breaches. Investigations will be initiated promptly and completed within one month of the breach being reported. The findings will be formally reported to the full Parish Council. Procedures are in place to detect, report and investigate a data breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the clerk will also notify those concerned directly.

- All staff, Councillors and volunteers are required to follow the Council's IT security protocols. In particular:
- It is strictly prohibited for unauthorised individuals to access the council IT system using another person's login details
- Users must not allow others to access equipment while logged in under their accounts
- IT systems must not be used in any manner that could compromise the security, integrity or reputation of the Council

Failure to comply with these requirements may result in disciplinary action.

Privacy Statement and Privacy Notices

Being transparent and providing accessible information to individuals about how the Council uses personal data is a fundamental requirement of data protection legislation. The primary method for providing this information is through a privacy statement, which explains how the Council uses and manages personal data. This will include:

- What personal information the council collects and processes
- How that information may be shared, including circulation to and between councillors where appropriate
- How the information is stored and protected
- The legal rights of individuals in relation to their personal data

Privacy notices will be used occasionally where data is collected for specific purposes (for example, allotment holders, event participation or consultation). Each notice will:

- Clearly state the name and contact details of the data controller
- Explain the specific purpose(s) for which the data is being collected
- Identify the lawful basis for processing
- Specify how long the data will be retained
- Advise the individual's right to withdraw their agreement where applicable

The issuing of a privacy notice will be recorded as part of the Information Audit kept by the council. The council will adopt a standard privacy notice template, however, these may be changed where necessary to reflect specific circumstances, for example, where data involving children is involved. In such cases, additional care will be taken to ensure that information is presented in a way that is appropriate and

understandable. Where consent is being relied on as the lawful basis for processing the data, privacy notices must contain a positive opt-in and be verifiable.

Information Audit

The Clerk as the Council's designated data management lead, will be responsible for carrying out, and maintaining an information audit which will detail what personal data it holds, how it is used, where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change annually with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity.

Individuals' Rights

Data protection legislation gives individuals the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- Tight to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling.

If a request is received to access or delete information, then the Clerk must respond to this request within a month. The Clerk has the delegated authority from the Council to deal with such requests. If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. The Council will be informed of such requests and will determine the charge.

Children

The UK GDPR provides special protection for the personal data of a child. The age when a child can give their own consent is 13 years of age. If the council collects data from young people under 13 years old, the council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children aged 13 plus, must be written in language that they will understand.

Summary

The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- A privacy statement will be available on the council's website and reference to it will be made in all emails sent from the council's email address.

- Privacy notices will be issued where appropriate.
- Data Protection will be included in the Council's risk assessment.
- The full council manages the process. All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

Reviewed April 2026 For review April 2029