Witham Town Council: UK GDPR Policy

This Policy sets out how the Council complies with UK data protection law, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and provides a framework for the management of personal data across the Council.

Policy overview, scope and purpose

Witham Town Council ("the Council") is committed to protecting the privacy and security of personal data that it processes in the course of delivering its functions and services.

This Policy applies to all personal data processed by or on behalf of the Council, regardless of the format, and to all councillors, employees, agency staff, volunteers, contractors and other third parties who process personal data on the Council's behalf.

This Policy should be read alongside the Council's General Privacy Notice, Public CCTV Policy, IT and Email Policy, Internal IT Policy, Data Retention Policy, Complaints Procedure and any other related policies adopted by the Council.

Legal framework

The Council will comply with all relevant data protection legislation and associated guidance, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000 and Environmental Information Regulations 2004, where applicable
- Relevant guidance and Codes of Practice issued by the Information Commissioner's Office (ICO) and other regulators

Roles and responsibilities

Data Controller

Witham Town Council is the Data Controller for all personal data that it processes in connection with its statutory functions, services and activities.

As Data Controller, the Council is responsible for deciding the purposes and means of processing personal data and for demonstrating compliance with data protection legislation.

Senior management and committee oversight

The Council has overall responsibility for:

- Approving this Policy and any significant amendments
- Ensuring appropriate resources and governance are in place to support compliance
- Receiving assurance, as required, on data protection risks and issues

Management responsibilities

The Town Clerk and senior officers are responsible for:

- Implementing this Policy and associated procedures within their areas of responsibility
- Ensuring that staff, councillors and contractors understand and comply with this Policy
- Ensuring appropriate technical and organisational measures are in place for systems and processes that handle personal data

Staff, councillors, volunteers and contractors

All councillors, employees, volunteers, agency staff and contractors who process personal data on behalf of the Council must:

- Familiarise themselves with this Policy and any related guidance
- Only process personal data where authorised and necessary for their role
- Keep personal data secure and confidential
- Report any actual or suspected personal data breach or security incident immediately in accordance with Council procedures

Failure to comply with this Policy may result in disciplinary or other appropriate action.

Data protection principles and accountability

The Council will comply with the data protection principles set out in Article 5 UK GDPR. Personal data will be:

1. Processed lawfully, fairly and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and, where necessary, kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for those purposes.
6. Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Council is responsible for, and will be able to demonstrate, compliance with these principles (the "accountability" principle).

Lawful bases for processing

The Council will only process personal data where one or more of the lawful bases in Article 6 UK GDPR apply. The main lawful bases relied upon by the Council are:

- Public task – where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Council.
- Legal obligation – where processing is necessary to comply with a legal obligation.
- Contract – where processing is necessary for the performance of a contract with the data subject or to take steps at their request before entering into a contract.
- Legitimate interests – in limited circumstances, where the Council or a third party has a legitimate interest and this is not overridden by the rights and freedoms of the individual.
- Consent – in specific cases where the individual has given clear consent for their personal data to be processed for one or more specified purposes.

For special category (sensitive) personal data, the Council will rely on one or more of the additional conditions in Article 9 UK GDPR and the Data Protection Act 2018, such as substantial public interest, employment and social protection law, or explicit consent.

Further information about the Council's lawful bases and conditions for processing different categories of personal data is provided in the General Privacy Notice.

Categories of data and purposes of processing

The Council processes a range of personal data necessary to carry out its statutory and discretionary functions. This may include, but is not limited to:

- Names, titles and aliases
- Contact details (addresses, email addresses, telephone numbers)
- Photographs and CCTV images
- Demographic and background information where relevant to services provided
- Financial information (e.g. bank details and transaction histories for payments, grants or fees)
- Information relating to Council services, consultations, complaints, bookings, events and civic functions

The Council's main purposes for processing personal data include:

- Delivering public services and facilities
- Managing Council assets, public spaces and events
- Responding to enquiries, requests, complaints and representations
- Fulfilling legal and regulatory obligations
- Administering grants, contracts and other agreements
- Operating CCTV systems for crime prevention and public safety
- Communicating with residents, stakeholders and partners

A fuller description of the categories of data processed and purposes is set out in the General Privacy Notice.

Information security and IT controls

The Council will apply appropriate technical and organisational measures to safeguard personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These measures include, but are not limited to:

- Use of up-to-date antivirus and firewall software on Council devices
- Secure server arrangements with controlled, permissions-based access to shared drives
- Strong password practices and account security measures
- Secure storage and transmission of sensitive and confidential data, including encryption where appropriate
- Access control to IT systems, email accounts, CCTV systems and other applications
- Regular backups of key systems and data, stored securely
- Separation of public and internal Wi-Fi networks
- Restrictions on installation of unauthorised software and devices
- Monitoring and review of IT and email usage in accordance with Council policies

Day-to-day information security arrangements are detailed in the IT and Email Policy and Internal IT Policy, which support this Policy and must be complied with by all users.

CCTV and other high-risk processing

The Council operates public CCTV systems for the prevention and detection of crime, protection of public safety and management of Council assets.

CCTV processing is governed by the Council's Public CCTV Policy, which sets out:

- The purposes for which CCTV is used and the legal basis for processing
- The locations and operation of cameras
- Access controls, monitoring and disclosure of recordings
- Data protection impact assessments and privacy considerations
- Retention and deletion of CCTV footage
- Provision of footage to law enforcement or other authorised bodies

Any other high-risk processing (for example, new surveillance technologies or large-scale processing) will be subject to appropriate risk assessments, including Data Protection Impact Assessments (DPIAs) where required.

Data sharing and processors

The Council may share personal data with other organisations where this is lawful, necessary and proportionate, for example:

- Other local authorities and public bodies (such as district and county councils)
- Government departments and agencies
- Law enforcement and regulatory bodies, including the Police
- Contractors, service providers and professional advisers
- Community and voluntary organisations working in partnership with the Council

Where the Council uses third parties to process personal data on its behalf ("processors"), appropriate contracts or data-sharing agreements will be in place to ensure that processors:

- Process personal data only on the Council's documented instructions
- Keep personal data secure
- Assist the Council in meeting its obligations in relation to data subject rights, breaches and DPIAs
- Delete or return personal data at the end of the contract as required

The Council will only share the minimum amount of personal data necessary for the purpose and will not sell personal data to third parties.

Data retention and disposal

The Council will not keep personal data for longer than is necessary for the purposes for which it was collected.

Retention periods for different categories of records are set out in the Council's Data Retention Policy and any associated schedules.

At the end of the applicable retention period, personal data will be securely deleted, destroyed or anonymised in accordance with Council procedures and any legal or regulatory requirements.

Data subject rights

Individuals whose personal data is processed by the Council ("data subjects") have a number of rights under UK GDPR, including:

- Right of access – to request a copy of their personal data and information about how it is used
- Right to rectification – to ask for inaccurate or incomplete data to be corrected
- Right to erasure – in certain circumstances, to request that their data is deleted
- Right to restrict processing – to request that processing is restricted in certain circumstances
- Right to object – to object to processing in certain circumstances, including some processing based on public task or legitimate interests
- Right to data portability – in certain circumstances, to have data transferred to another controller
- Right to withdraw consent – where processing is based on consent, to withdraw that consent at any time

Requests to exercise these rights should be made in writing to the Council using the contact details set out in the General Privacy Notice or on the Council's website.

The Council will respond to valid requests within the timescales set out in UK GDPR, normally within one month.

Further information on how to exercise these rights is provided in the General Privacy Notice.

Data breaches and incident handling

A personal data breach is a security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

All councillors, employees, volunteers and contractors must immediately report any suspected or confirmed personal data breach, or other information security incident, in accordance with Council procedures and to the appropriate senior officer.

The Council will:

- Investigate reported incidents promptly and take appropriate remedial action
- Maintain records of personal data breaches
- Assess the risks to individuals arising from a breach
- Notify the ICO and affected individuals where legally required

Witham town council

Data breach handling will be coordinated with the Council's IT and Email Policy, Internal IT Policy and any incident response procedures.

Training, awareness and monitoring

The Council will provide appropriate training and guidance on data protection and information security to councillors, employees and relevant third parties, proportionate to their roles and responsibilities.

The Council will promote awareness of this Policy and related privacy information so that staff, members and the public understand how personal data is used and protected.

Compliance with this Policy may be monitored through internal checks, audits or reviews, and any issues identified will be addressed through appropriate actions.

Adopted at meeting of Policy and Resources Committee Meeting held 29.6.2026
To be reviewed June 2028