HASLEMERE TOWN COUNCIL

DATA PROTECTION POLICY

Contents

1. Policy Statement

Haslemere Town Council ("the Council") is committed to protecting the privacy and rights of individuals and to processing personal data lawfully, fairly, securely and transparently.

The Council recognises its responsibilities under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. Smaller authorities are required to comply with data protection law and to process personal data with care and in accordance with data protection principles . The Practitioners' Guide also expects smaller authorities to implement a data protection policy, provide training, carry out data audits and secure personal data using appropriate technical and organisational measures .

This policy sets out the Council's approach to the collection, use, storage, sharing, retention and disposal of personal data.

2. Purpose

The purpose of this policy is to:

- ensure the Council complies with data protection legislation;
- protect the rights of councillors, staff, residents, electors, contractors, volunteers, service users and other individuals whose personal data the Council processes;
- provide a clear framework for councillors and staff handling personal data;
- reduce the risk of data breaches, misuse or unlawful disclosure; and
- support openness and accountability in the Council's administration.

3. Scope

This policy applies to:

- all councillors;
- all employees;
- casual workers and volunteers;
- contractors and consultants acting for or on behalf of the Council;
- members of committees or sub-committees where they process Council information; and
- all personal data processed by the Council, whether held electronically, on paper, in photographs, audio recordings, CCTV images, emails, forms or any other format.

This policy applies to personal data processed in connection with all Council functions, services, employment matters, governance, communications, allotments, burials, events, facilities, complaints, correspondence, procurement and any other lawful activity of the Council.

4. Definitions

For the purposes of this policy:

Personal data means any information relating to an identified or identifiable living individual.

Special category data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, and data concerning a person's sex life or sexual orientation.

Processing means any operation carried out on personal data, including collecting, recording, storing, using, sharing, amending, deleting or destroying it.

Data subject means the individual the personal data relates to.

Data controller means the organisation that determines the purposes and means of processing personal data.

Processor means a person or organisation that processes personal data on behalf of the controller.

Personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. Roles and Responsibilities

5.1 The Council

The Council is responsible for ensuring that personal data is processed in compliance with legal requirements and good practice.

5.2 The Clerk

The Clerk, as the Council's proper officer, is responsible for the day-to-day implementation of this policy and for ensuring that:

- appropriate procedures are in place;
- privacy information is issued where required;
- records of processing are maintained;
- subject rights requests are managed;
- breaches are recorded and escalated appropriately; and
- staff and councillors receive appropriate guidance and training.

5.3 Data Protection Officer / Data Protection Support

The Council will maintain access to competent data protection advice and oversight, whether through an appointed Data Protection Officer or other suitable arrangement consistent with legal requirements and the Council's circumstances. The Practitioners' Guide states that smaller authorities should appoint a Data Protection Officer to oversee compliance with GDPR .

5.4 Councillors, Staff and Others

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

- comply with this policy and related procedures;

- only access personal data where necessary;
- keep personal data secure and confidential;
- report any actual or suspected breach immediately; and
- complete any required training.

6. Data Protection Principles

The Council will comply with the core data protection principles. Personal data must be:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes**
3. **Adequate, relevant and limited to what is necessary**
4. **Accurate and, where necessary, kept up to date**
5. **Kept for no longer than necessary**
6. **Processed securely**, using appropriate technical and organisational measures

Smaller authorities must process personal data with care and in line with these principles .

The Council will also comply with the principle of **accountability**, meaning it will be able to demonstrate compliance through policies, procedures, records and practice.

7. Lawful Basis for Processing

The Council will identify and document an appropriate lawful basis before processing personal data.

Depending on the activity, the Council may rely on one or more of the following lawful bases:

- **Legal obligation**
- **Public task**
- **Contract**
- **Consent**
- **Vital interests**
- **Legitimate interests**, where applicable and lawful

Where the Council processes special category data, it will identify both:

- an Article 6 lawful basis; and
- an appropriate Article 9 condition or other relevant legal condition.

Where required by the Data Protection Act 2018, the Council will maintain an **appropriate policy document** explaining compliance procedures and retention/erasure arrangements for such processing .

8. Fair Processing and Privacy Notices

The Council will provide privacy information in a clear and accessible form. Privacy notices will explain, as appropriate:

- the identity and contact details of the Council;
- the contact details for data protection queries;
- the purposes of processing;
- the lawful basis for processing;
- categories of personal data processed;
- who personal data may be shared with;
- whether data will be transferred outside the UK;
- how long data will be retained;
- the rights available to individuals; and
- the right to complain to the Information Commissioner's Office (ICO).

Privacy notices will be issued at the point personal data is collected, or as soon as reasonably practicable afterwards.

9. Data Minimisation and Accuracy

The Council will only collect personal data that is necessary for a specified purpose. It will not collect excessive or irrelevant information.

Reasonable steps will be taken to ensure personal data is accurate and kept up to date. Inaccurate or outdated data will be corrected or deleted without undue delay where appropriate.

10. Retention and Disposal

The Council will not keep personal data for longer than is necessary. Personal data will be retained in accordance with the Council's **Retention Schedule** or, where no schedule exists, only for as long as is reasonably necessary for the purpose for which it was collected.

When retention periods expire, personal data will be securely deleted, destroyed or anonymised.

Where an appropriate policy document is required, this must explain the Council's retention and erasure approach and give an indication of likely retention periods .

11. Information Security

The Council will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

These measures will include, where appropriate:

- password protection and strong authentication;

- access controls based on role and need;
- secure Council email accounts;
- secure storage of paper records;
- encryption on devices and removable media where appropriate;
- anti-virus, patching and backup arrangements;
- secure transfer methods for sensitive information;
- confidential waste disposal and shredding;
- locking of offices, cabinets and devices;
- screen-locking and clear desk practices; and
- controlled use of cloud systems and third-party suppliers.

The Practitioners' Guide emphasises secure handling, data audits, training, and appropriate measures to protect personal data, and identifies authority-owned email accounts and an IT policy as good practice for accountability and security .

12. Use of Email, Systems and Devices

Council business must be carried out using approved Council systems wherever possible.

Councillors and staff must:

- use Council-issued or approved email accounts for Council business wherever available;
- avoid using personal email accounts for official Council business unless expressly authorised and subject to security controls;
- ensure personal devices used for Council business are protected by password, kept updated and used securely;
- not forward Council personal data to unsecured accounts or devices; and
- take care when sending emails, especially where attachments contain personal data.

The Council will maintain an IT policy to support secure and lawful use of equipment and software, reflecting sector guidance for smaller authorities .

13. Data Sharing

The Council may share personal data where there is a lawful basis and where sharing is necessary, proportionate and secure.

Personal data may be shared with:

- other public bodies;
- regulators or auditors;

- insurers, legal advisers or professional advisers;
- contractors and service providers acting on the Council's behalf; or
- law enforcement or safeguarding bodies,

provided the sharing is lawful and appropriately documented.

Where third parties process data on behalf of the Council, the Council will ensure suitable contractual and security arrangements are in place.

14. Special Category Data and Criminal Offence Data

The Council recognises that some processing involves more sensitive information, such as employment records, health information, equality monitoring data, safeguarding records or other special category data.

Where the Council processes special category data or criminal offence data, it will:

- identify the relevant lawful basis and condition;
- ensure the processing is necessary and proportionate;
- keep access restricted to those who need it;
- apply higher standards of confidentiality and security; and
- maintain an appropriate policy document where required by the Data Protection Act 2018 .

15. Individual Rights

The Council will respect the rights of individuals under data protection law, including:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure, where applicable;
- the right to restrict processing;
- the right to data portability, where applicable;
- the right to object; and
- rights in relation to automated decision-making and profiling, where applicable.

Any person wishing to exercise their rights should contact the Clerk in the first instance. Requests will be handled in accordance with statutory timescales and legal requirements.

16. Subject Access Requests

Individuals are entitled to request confirmation that their personal data is being processed and to request access to that data, subject to any exemptions.

The Council will:

- log requests on receipt;
- verify identity where appropriate;
- respond within the statutory timeframe (one month of receipt);
- provide information in an accessible form unless an exemption applies; and
- keep a record of requests and outcomes.

17. Personal Data Breaches

Any actual or suspected personal data breach must be reported to the Clerk immediately.

The Council will:

- investigate and assess the breach promptly;
- take steps to contain and recover from the incident;
- record the facts, effects and remedial action taken;
- notify the ICO where required within 72 hours of becoming aware of a reportable breach; and
- notify affected individuals where required by law.

Failure to report a breach internally may itself be treated as a serious matter.

18. Data Protection by Design and by Default

The Council will consider data protection at the outset of new projects, services, systems and processes. This includes considering:

- whether personal data is actually needed;
- what minimum data is necessary;
- who will have access;
- how long the data should be retained;
- what privacy information is needed; and
- whether any higher-risk processing requires further assessment.

19. Training and Awareness

The Council will ensure that all councillors and staff receive appropriate data protection training and guidance relevant to their role. Refresher training will be provided periodically and when legal or procedural changes occur.

Regular training is identified as a key expectation for smaller authorities in the Practitioners' Guide .

20. Records Management and Audit

The Council will maintain appropriate records of processing activities and will periodically review:

- what personal data is held;
- why it is held;
- where it is stored;
- who has access;
- whether retention remains appropriate; and
- whether security measures remain effective.

Regular data audits are identified as good practice for smaller authorities .

21. Related Policies and Documents

This policy should be read alongside the Council's:

- Privacy Notice(s)
- Retention Schedule / Retention and Disposal Policy
- Information Security / IT Policy
- Data Breach Procedure
- Subject Access Request Procedure
- Records Management Policy
- Publication Scheme
- Social Media Policy
- CCTV Policy, where applicable
- Employee Privacy Notice, where applicable

22. Monitoring and Review

This policy will be reviewed:

- annually;
- following any material change in legislation or ICO guidance;

- following any significant data breach or compliance issue; or
- when the Council introduces new systems or processing activities requiring amendment.

Any amendments must be approved by the Council or the relevant committee in accordance with the Council's governance arrangements.

23. Contact Details

For queries about this policy or data protection matters, contact:

Clerk / Responsible Officer:
Lisa O'Sullivan, Town Hall, High Street, Haslemere GU27 2HG

Town.clerk@haslemere-tc.gov.uk

01428 654305

Data Protection Officer / Data Protection Contact:
Lisa O'Sullivan, Town Hall, High Street, Haslemere GU27 2HG

Town.clerk@haslemere-tc.gov.uk

01428 654305

Information Commissioner's Office:
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Website: www.ico.org.uk