DATA PROTECTION & PRIVACY POLICY

Contents

This Data Protection and Privacy Policy was adopted by the council at its meeting held on 20th May 2025.

DATA PROTECTION POLICY

1. OVERVIEW

The Council is committed to being transparent about how it collects and uses personal data, and to meeting our data protection obligations. This policy sets out the Council's commitment to data protection, and your rights and obligations in relation to personal data in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).

The council will follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners, or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the legislation.

The Council has appointed the Executive Officer as the person with responsibility for data protection compliance within the Council. Questions about this policy, or requests for further information, should be directed to them.

2. STATEMENT OF POLICY

In order to operate efficiently, the Town Council has to collect and use information about people with whom it works. These may include members of the public, current, past, and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded, and used, and whether it be on paper, in computer records or recorded by any other means there are safeguards within the legislation to ensure this.

The Town Council regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly.

To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the UK GDPR and Data Protection Act 2018.

3. DEFINITIONS

"Personal data" is any information that relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information. It includes both automated personal data and manual filing systems where personal data are accessible according to specific criteria. It does not include anonymised data.

"Processing" is any use that is made of data, including collecting, recording, organising, consulting, storing, amending, disclosing, or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic or biometric data as well as criminal convictions and offences.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

"Data controller" means the person or organisation that determines when, why and how to process personal data. The Council is the data controller of all personal data used in its business.

"Data subject" means a living, identified or identifiable individual about whom the Council holds personal data.

"Data processor" means any person or organisation that processes personal data on behalf of a data controller.

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

4. DATA PROTECTION PRINCIPLES

The UK GDPR sets out seven key principles that the Council must comply with when processing personal data:

1. **Lawfulness, fairness and transparency**: Personal data shall be processed lawfully, fairly and in a transparent manner.
2. **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. **Data minimisation**: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date.
5. **Storage limitation**: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Integrity and confidentiality (security)**: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. **Accountability**: The data controller shall be responsible for, and be able to demonstrate compliance with the UK GDPR.

5. LAWFUL BASES FOR PROCESSING

The Council will only process personal data where it has a lawful basis for doing so. Under the UK GDPR, there are six available lawful bases for processing:

1. **Consent**: The individual has given clear consent for the Council to process their personal data for a specific purpose.
2. **Contract**: The processing is necessary for a contract the Council has with the individual, or because they have asked the Council to take specific steps before entering into a contract.
3. **Legal obligation**: The processing is necessary for the Council to comply with the law (not including contractual obligations).

4. **Vital interests**: The processing is necessary to protect someone's life.

5. **Public task**: The processing is necessary for the Council to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

6. **Legitimate interests**: The processing is necessary for the Council's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform official tasks, so councils need to rely on the public task basis instead.)

For local councils, the lawful basis most commonly relied upon is 'public task' (6(1)(e) of UK GDPR) as most of the council's processing is done to perform tasks for which it has statutory powers or duties.

6. PROCESSING PERSONAL DATA

The Council will process personal data (that is not classed as special categories of personal data) in accordance with our obligations under the UK GDPR for one or more of the following lawful bases:

- it is necessary for the performance of a contract, e.g., an employment contract
- it is necessary to comply with a legal obligation
- it is necessary to perform a task in the public interest or in the exercise of official authority vested in the controller
- it is necessary to protect the vital interests of a data subject or another person

If the Council processes personal data in line with one of the above bases, it does not require consent. Otherwise, the Council is required to gain your consent to process your personal data.

If the Council asks for your consent to process personal data, then we will explain the reason for the request. You do not need to consent or can withdraw consent later.

The Council will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

7. SPECIAL CATEGORIES OF DATA

The Council will only process special categories of personal data (see definition above) on the following bases in accordance with UK GDPR Article 9:

- where it is necessary for carrying out rights and obligations under employment law or a collective agreement
- where it is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent
- where the data has been made public by the data subject
- where it is necessary for the establishment, exercise or defence of legal claims

- where it is necessary for reasons of substantial public interest based on law which is proportionate to the aim pursued and which contains appropriate safeguards
- where it is necessary for reasons of public interest in public health
- where it is necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the Council processes special categories of personal data in line with one of the above bases, it does not require consent. In other cases, the Council is required to gain explicit consent to process special categories of personal data.

If the Council asks for your consent to process a special category of personal data, then we will explain the reason for the request, and you do not have to consent or can withdraw consent later.

8. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

The Council will conduct Data Protection Impact Assessments for any new processing that is likely to result in a high risk to individuals' rights and freedoms. This might include:

- New technologies or systems that collect, use or store personal data
- Systematic monitoring of public areas on a large scale
- Processing special categories of data on a large scale
- Processing data relating to vulnerable subjects (including children)

The DPIA will:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

The Executive Officer will be responsible for ensuring that DPIAs are conducted when required.

9. INDIVIDUAL RIGHTS

As a data subject, individuals have several rights in relation to their personal data under the UK GDPR:

Subject Access Requests
Individuals have the right to make a subject access request. If an individual makes a subject access request, the Council will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the United Kingdom and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided)

- their rights to rectification or erasure of data, or to restrict or object to processing
- their right to complain to the Information Commissioner if they think the Council has failed to comply with their data protection rights
- whether or not the Council carries out automated decision-making and the logic involved in any such decision-making.

The Council will also provide the individual with a copy of their personal data undergoing processing. This will normally be in electronic form if they have made a request electronically unless they agree otherwise. If additional copies are requested, the Council may charge a fee, which will be based on the administrative cost to the Council of providing the additional copies.

To make a subject access request, individuals should send the request to the Executive Officer or Chairman of the Council. In some cases, the Council may need to ask for proof of identification before the request can be processed. The Council will inform the individual if it needs to verify their identity and the documents required.

The Council will normally respond to a request within a period of one calendar month from the date the request is received. Where the Council processes large amounts of the individual's data, this may not be possible within one month. The Council will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. If the Council believes a request is manifestly unfounded or excessive, it will either:

- respond and explain why it considers the request to be manifestly unfounded or excessive, or
- charge a reasonable fee reflecting the administrative costs of providing the information, or
- refuse to respond

A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Council has already responded. If an individual submits a request that is unfounded or excessive, the Council will notify them that this is the case and whether or not it will respond to it.

Other Rights

Individuals have several other rights in relation to their personal data. They can require the Council to:

- rectify inaccurate data
- stop processing or erase data that is no longer necessary for the purposes of processing
- stop processing or erase data if the individual's interests override the Council's legitimate grounds for processing data (where the Council relies on its legitimate interests as a reason for processing data)
- stop processing or erase data if processing is unlawful

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Council's legitimate grounds for processing data.

To ask the Council to take any of these steps, the individual should send the request to the Executive Officer or Chairman of the Council.

Individuals also have the right to:

- withdraw consent for processing at any time (where consent is the lawful basis)
- object to processing based on legitimate interests or the performance of a task in the public interest
- object to direct marketing
- not be subject to automated decision-making including profiling
- complain to the Information Commissioner's Office (ICO)

10. DATA SECURITY

The Council takes the security of personal data seriously. The Council has controls in place to protect personal data against loss, accidental destruction, misuse, or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Council engages third parties to process personal data on our behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Paper Storage:

- When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- Data printouts should be shredded and disposed of securely when no longer required.

Electronic Storage:

- Data stored electronically 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 between employees.
- Multi-factor authentication should be used where available.
- If data is stored on removable media (like a USB drive), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with the Council's standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

11. DATA BREACHES

The Council has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur the Council must take notes and keep evidence of that breach.

If any Council member or employee is aware of a data breach they must contact the Executive Officer or Chairman of the Council immediately and keep any evidence they have in relation to the breach.

If the Council discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

The Council will record all data breaches regardless of their effect in a data breach register. If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures the Council has taken.

12. INTERNATIONAL DATA TRANSFERS

Following the UK's exit from the European Union, the Council will not transfer personal data outside the UK unless such transfers are covered by appropriate safeguards or exemptions under UK data protection law.

The UK has established adequacy arrangements with the EEA, allowing data flows to continue without additional safeguards. For transfers to other countries, appropriate safeguards must be put in place, such as:

- Standard Contractual Clauses approved by the Secretary of State
- Binding Corporate Rules
- Codes of Conduct or Certification Mechanisms
- Derogations for specific situations (such as explicit consent)

The Council will consult legal advice before transferring personal data outside the UK to countries not covered by UK adequacy arrangements.

13. INDIVIDUAL RESPONSIBILITIES

Those covered by this policy are responsible for helping the Council keep their personal data up to date. They should let the Council know if data provided to the Council changes, for example if they move to a new house or change bank details.

Everyone who works for, or on behalf of, the Council has responsibility for ensuring data is collected, stored, and handled appropriately, in line with the Council's policies.

Officers and Members may have access to the personal data of other individuals and of members of the public in the course of their work with the Council. Where this is the case, the Council relies on them to help meet data protection obligations to staff and members of the public.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes
- not to disclose data except to individuals (whether inside or outside the Council) who have appropriate authorisation
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, locking computer screens when away from desk, and secure file storage and destruction including locking drawers and cabinets, not leaving documents on desk whilst unattended)
- not to remove personal data, or devices containing or that can be used to access personal data, from the Council's premises without prior authorisation and without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device
- not to store personal data on local drives or on personal devices that are used for work purposes
- to never transfer personal data outside the United Kingdom except in compliance with the law and with express authorisation from the Executive Officer or Chair of the Council
- to ask for help from the Council's data protection lead if unsure about data protection or if they notice a potential breach or any areas of data protection or security that can be improved upon.

Failing to observe these requirements may amount to a disciplinary offence or a Code of Conduct Complaint, which will be dealt with under the Council's disciplinary procedure or appropriate Member Services.

Significant or deliberate breaches of this policy, such as accessing personal data without authorisation or a legitimate reason to do so or concealing or destroying personal data as part of a subject access request, may constitute gross misconduct and could lead to dismissal without notice.

14. DATA CONTROLLERS AND PROCESSORS

The Data Controller Ashington Town Council is the data controller for all personal data processed by the Council.

The Data Protection Lead The Executive Officer serves as the Data Protection Lead for the Council. The responsibilities of this role include:

- Keeping the Council updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Ensuring data protection training and advice is provided to Members and staff

- Serving as the first point of contact for data protection matters
- Handling data subject requests and data breaches

Data Protection Officer As a public authority, the Council must designate a Data Protection Officer (DPO), as required by UK GDPR. The Executive Officer has been designated as the Council's DPO. The DPO's responsibilities include:

- Informing and advising the Council about obligations under data protection laws
- Monitoring compliance with data protection laws
- Providing advice regarding Data Protection Impact Assessments
- Being the point of contact for the Information Commissioner's Office

The Data Processors Council Officers act as data processors when handling personal data on behalf of the Council.

15. PRIVACY NOTICES

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. As such, the Council will provide privacy notices that are concise, transparent, intelligible, easily accessible, and written in clear and plain language.

The Council's privacy notices will include:

- Identity and contact details of the data controller (the Council)
- Contact details of the Data Protection Officer/Lead
- Purpose of the processing and the lawful basis for it
- The legitimate interests for the processing (if applicable)
- Categories of personal data obtained (if not obtained directly from the individual)
- Recipients or categories of recipients of the personal data
- Details of transfers of personal data to countries outside the UK (if applicable)
- Retention period or criteria used to determine the retention period
- Rights available to individuals in respect of the processing
- Right to withdraw consent (if applicable)
- Right to lodge a complaint with the ICO
- Details of automated decision making, if applicable
- Source of the personal data (if not obtained directly from the individual)

The Council's general Privacy Notice is available on the Council website and will be reviewed annually.

16. DATA INVENTORY AND PROCESSING ACTIVITIES

The Council maintains a data inventory that records:

- Types of personal data held
- Categories of data subjects
- Processing activities
- Processing purposes
- Legal basis for processing
- Retention periods
- Technical and organisational security measures

This inventory is reviewed annually to ensure it remains accurate and up to date.

17. REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The Information Commissioner maintains a public register of data controllers. The Town Council is registered as such.

The Data Protection Act 2018 requires every data controller who is processing personal data to register and renew their notification with the ICO on an annual basis. Failure to do so is a criminal offence.

The Data Protection Officer/Lead will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Data Protection Officer/Lead immediately.

18. DATA RETENTION SCHEDULE

GENERAL

DOCUMENT	**MINIMUM RETENTION PERIOD**	**REASON**
Signed Minutes	Indefinite	Archive/Public Inspection
Agendas	5 years	Management
Title Documents/Deeds	Indefinite	Audit/Management
Contracts/Leases	Indefinite or 6 years after contract end	Management/Limitation Act
E-Mail (Excluding Spam)	2 years	Local Choice

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Register of Member's Interests	Term of office + 1 year	Local Choice
Strategic Plans/Annual Reports	Permanent Archive once superseded	Common Practice
Policies & Operational Procedures	7 years after superseded	Local Choice
Legal/Litigation Files	Active + 7 years	Local Choice
Debt Recovery Matters	Active + 2 years	Local Choice
Complaints Records	6 years	Common Practice
Planning applications and related documents	1 year after decision	Management
Allotment registers and plans	Indefinite	Audit/Management

FINANCIAL

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Audited Accounts	Indefinite	Archive/Public Inspection
Accounting Records (Invoices/VAT records etc)	6 years	VAT
Bank Statements, Cheque Books, Paying-In Books	Last Completed Audit Year + 6 years	Audit/VAT
Insurance Company Records	Indefinite	Management
Insurance Policies	Whilst Valid + 6 years	Management
Employer's Liability Certificates	40 years from commencement/renewal	Statute
Budgets	Indefinite	Management
Quotations & Tenders	6 years	Limitations Act
Payroll Records	12 years	Superannuation/Pension

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Grant applications	6 years	VAT/Audit

EMPLOYMENT

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Timesheets	7 years	Personal Injury
Recruitment Documents	5 years	Local Choice
Documents on Persons not hired	1 year	Equal Opportunities Claims
Accident or Injury at Work	7 years	Local Choice
Personnel Administration	6 years after person leaves council	Local Choice & Statutory
Personnel Service Records	Indefinite	Local Choice
Training records	Current year + 6 years	Management
Disciplinary proceedings	Oral warning: 6 months Written warning - level 1: 6 months Written warning - level 2: 12 months Final warning: 18 months	Local Choice

19. MONITORING AND REVIEW OF THIS POLICY

The Executive Officer shall be responsible for reviewing this policy annually to ensure that it meets legal requirements and reflects best practice.

Any proposed amendments to this policy shall be reported to and approved by the Council.