Data Protection Policy

Including Privacy Notice and Retention Schedule

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 General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

The council will therefore 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 Act.

The Council has appointed the Town Clerk 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 in order 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 Act to ensure this.

The Town Council regards the lawful and correct treatment of personal information as very important 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 Data Protection Act 1998.

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 proceeding.

4. DATA PROTECTION PRINCIPLES

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met

2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed

4. Shall be accurate and where necessary, kept up to date

5. Shall not be kept for longer than is necessary for that purpose or those purposes

6. Shall be processed in accordance with the rights of data subjects under the Act

7. Shall be kept secure i.e. protected by an appropriate degree of security

8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual

Special categories of personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions

5. PROCESSING PERSONAL DATA

The Council will process your personal data (that is not classed as special categories of personal data) for one or more of the following reasons:

- ✓ it is necessary for the performance of a contract, e.g., your contract of employment (or services)
- ✓ it is necessary to comply with any legal obligation

- ✓ it is necessary the Council's legitimate interests (or for the legitimate interests of a third party), unless there is a good reason to protect your personal data which overrides those legitimate interests
- ✓ it is necessary to protect the vital interests of a data subject or another person
- ✓ it is necessary for the performance if a task carried out in the public interest or in the exercise of official authority vested in the controller.

If the Council processes your personal data (excluding special categories of personal data) in line with one of the above bases, it does not require your 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.

6. SPECIAL CATEGORIES OF DATA

The Council will only process special categories of your personal data (see above) on the following basis in accordance with legislation:

- ✓ where it is necessary for carrying out rights and obligations under employment law or a collective agreement
- ✓ where it is necessary to protect your vital interests or those of another person where you are physically or legally incapable of giving consent
- ✓ where you have made the data public
- ✓ where it is necessary for the establishment, exercise, or defence of legal claims
- ✓ where it is necessary for the purposes of occupational medicine or for the assessment of your working capacity
- ✓ where it is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates to only members or former members provided there is no disclosure to a third party without consent
- ✓ where it is necessary for reasons for substantial public interest on the basis of law which is proportionate to the aim pursued and which contains appropriate safeguards
- ✓ where is it necessary for reasons of public interest in the area of public health
- ✓ where is it necessary for archiving purposes in the public interest or scientific and historical research purposes.

If the Council processes special categories of your personal data in line with one of the above bases, it does not require your consent. In other cases, the Council is required to gain your consent to process your 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. You do not have to consent or can withdraw consent later.

7. INDIVIDUAL RIGHTS

As a data subject, you have several rights in relation to your personal data.

SUBJECT ACCESS REQUESTS

You have the right to make a subject access request. If you make a subject access request, the Council will tell you:

- whether or not your 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 yourself;
- to whom your data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long your personal data is stored (or how that period is decided)
- your rights to rectification or erasure of data, or to restrict or object to processing
- your right to complain to the Information Commissioner if you think the Council has failed to comply with your 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 you with a copy of your personal data undergoing processing. This will normally be in electronic form if you have made a request electronically unless you agree otherwise. If you want additional copies, 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, you should send the request to the Clerk 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 you if we need to verify your identity and the documents we require.

The Council will normally respond to a request within a period of one month from the date it is received. Where the Council processes large amounts of your data, this may not be possible within one month.

The Council will write to you within one month of receiving the original request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, the Council is not obliged to comply with it. Alternatively, the Council can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. 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 you submit a request that is unfounded or excessive, the Council will notify you that this is the case and whether or not we will respond to it.

OTHER RIGHTS

You have several other rights in relation to your personal data. You 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 your interests override the Council's legitimate grounds for processing data (where the Council relies on our 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 your interests override the Council's legitimate grounds for processing data.

- complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk).

To ask the Council to take any of these steps, you should send the request to the Clerk or Chairman of the Council.

8. DATA STORAGE AND 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 on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

- 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.
- When data is stored electronically, it 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.
- If data is stored on removable media (like a CD or DVD), 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 an 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.

DATA BREACHES

The Council have 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 you are aware of a data breach you must contact the Clerk or Chairman of the Council immediately and keep any evidence, you have in relation to the breach. If the Council discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of yourself, we will report it to the Information Commissioner within 72 hours of discovery.

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

INTERNATIONAL DATA TRANSFERS

The Council will not transfer personal data to countries outside the EEA.

9. 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 some 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 you 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 European Economic Area except in compliance with the law and with express authorisation from the Clerk or Chair of the Council
- to ask for help from the Council's data protection lead if unsure about data protection or if you 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 of 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.

10. NOTIFICATION TO THE INFORMATION COMMISSIONER

The Information Commissioner maintains a public register of data controllers.

The Town Council is registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The Data Protection Officer 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 Information Officer immediately.

11. PRIVACY NOTICE – TRANSPARENCY OF DATA PROTECTION

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

What information is being collected?	
Who is collecting it?	The Council
How is it collected?	Electronically, hard copies, orally
Why is it being collected?	To carry out the legitimate functions and powers of the Council: The Council is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the Council's statutory functions and powers. Sometime when exercising these powers or duties it is necessary to process personal data of residents or people using the Council's services. We will always consider your interests and rights. We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.
How will it be used?	For Council purposes, in the exercise of official authority, to perform a task that is in the public interest and that is set out in law.
Who will it be shared with?	Authorised third parties.
The Data Controller	Ashington Town Council
The Data Information Officers	Town Clerk
The Data Processors	Council Officers
The Data Protection Officer	The Clerk
The Data Controller	Ashington Town Council
Retention period	Refer to the Councils Retention Schedule below

12. 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	Management
E-Mail (Excluding Spam)	2 years	Local Choice
Register of Member's Interests	1 year after end of service	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

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	Audit
Insurance Company Records	Indefinite	Management
Insurance Policies	Whilst Valid	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

EMPLOYMENT

DOCUMENT	MINIMUM RETENTION PERIOD	REASON
Timesheets	7 years	Personal Injury
Recruitment Documents	5 years	Local Choice
Documents on Persons not hired	1year	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