

MIDDLEWICH TOWN COUNCIL

DATA PROTECTION AND RETENTION POLICY



Purpose	2
Definitions	2
Data protection principles	2
Privacy Notes	3
Processing	3
Personal Data of Employees	4
Individual rights	5
Data security	6
Training	8
Data Retention	8
Annex A - Data Retention Schedule	9



Purpose

The council is committed to being transparent about how it collects and uses the personal data of staff, 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).

This policy applies to all data collected and held by the Council. 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.

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 protection principles

The council processes data in accordance with the following data protection principles the council:

- processes personal data lawfully, fairly and in a transparent manner
- collects data only for specified, explicit and legitimate purposes and does not process data in a manner incompatible with those purposes
- processes data only where it is adequate, relevant and limited to what is necessary for the purposes of processing
- keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- keeps personal data only for the period necessary for processing



- adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

The council will tell you of the personal data it processes, the reasons for processing your personal data, how we use such data, how long we retain the data, and the legal basis for processing in our privacy notices.

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. The council will not process your personal data if it does not have a legal basis for processing.

The council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

Privacy Notes

The Town Clerk shall prepare Privacy Notices as required which will be published on the Town Council website. They shall be reviewed at least annually. Privacy Notices may vary depending on the data being collected/held.

The Town Council will use a blended approach to provide privacy information to individuals; providing information at the point of collection and reference to the full Privacy Notice where it is not practical to provide the notice in full at the point of collection.

At collection sufficient information will be given to detail why the data is being collected, how it will be used, how long it will be kept for and whether it will be shared with any third party.

Privacy Notices will be prepared with reference to guidance from the Information Commissioner's Office and shall be provided in simple language in a clear font.

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); and/or
- it is necessary to comply with any legal obligation; and/or
- it is necessary for 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; and/or
- it is necessary to protect the vital interests of a data subject or another person; and/or
- it is necessary for the performance of 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.

Personal Data of Employees

Personal data gathered during employment is held in your personnel file in hard copy and electronic format on HR and IT systems and servers. The periods for which the council holds your HR-related personal data are contained in our privacy notices to individuals.

Sometimes the council will share your personal data with contractors and agents to carry out our obligations under a contract with the individual or for our legitimate interests. We require those individuals or companies to keep your personal data confidential and secure and to protect it in accordance with Data Protection law and our policies. They are only permitted to process that data for the lawful purpose for which it has been shared and in accordance with our instructions.

The council will update HR-related personal data promptly if you advise that your information has changed or is inaccurate. You may be required to provide documentary evidence in some circumstances.

The council keeps a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

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 it is necessary for reasons of public interest in the area of public health; and
- where it is 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.

Individual rights

As a data subject, you have a number of 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; and
- 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 Town Clerk. 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 a number of 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; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not 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 Town Clerk.

Data security

The council takes the security of personal data seriously. The council has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by authorised 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.



Data breaches

A data breach is defined as a breach of security leading to '*accidental or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*'

The Town Clerk shall maintain procedures to safeguard against potential data breaches.

All data breaches shall be reported to the Town Clerk who shall maintain a record of data breaches and determine, in accordance with Information Commissioner's Office guidance whether the breach must be notified.

International data transfers

The council will not transfer HR-related personal data to countries outside the EEA.

Individual Employee responsibilities

You are responsible for helping the council keep your personal data up to date. You should let the council know if data provided to the council changes, for example if you move to a new house or change your 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.

You may have access to the personal data of other individuals and of members of the public in the course of your work with the council. Where this is the case, the council relies on you to help meet our 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; and
- 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, which will be dealt with under the council's disciplinary procedure. 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.

Training

All members and employees of the council shall receive an induction on Data Protection and training as required.

The Town Clerk shall maintain a guidance note on Data Protection for both members and employees to provide easy to access guidance on Data Protection practices.

Data Retention

The Town Council will only keep data for as long as it is necessary to do so. The council's standard data retention requirements are detailed in Annex A.

Data (electronic or physical) should only be disposed of if reviewed in accordance with the following:

- a. Is retention required to fulfil a statutory or regulatory requirement?
- b. Is retention required to meet the operational needs of a service?
- c. Is retention required to evidence events in the case of dispute?
- d. Is retention required because the document/record is of historic interest or intrinsic value?

All records containing personal information must be destroyed at the end of the retention period.

Where documents are of historical interest it may be appropriate that they are transmitted to the County Records Office or the Middlewich Heritage Trust.

Retention periods may be increased by government regulation, judicial or administrative constraint order, contract, pending litigation or audit requirements and such modifications shall supersede the requirements in Annex A.

This is a non-contractual policy and procedure which will be reviewed from time to time.

Date of policy: March 2020

Approving committee:

Date of committee meeting:

Policy version reference:

Policy effective from:

Date for next review:



Annex A: Data Retention Schedule

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
Email (excluding SPAM)	3 years	Local Choice
Register of Members Interests	1 year after end of Service	Local Choice
Members Allowances Register	6 years	Tax, Limitation Act
Strategic Plans, Annual Reports etc	Permanent Archive once superseded	Common Practice
Polices and Operational Procedures	7 years after superseded	Local Choice
Legal / Litigation Files	Active + 7 years	Local Choice, Limitation Act
Commercial Debt Recovery Matters	Active + 6 years	Management, Limitation Act
Complaints Records	Active + 6 years	Common Practice, Limitation Act
Audited Accounts	Indefinite	Archive, Public Inspection
Accounting Records (invoices, VAT records etc)	6 years	VAT
Bank Statements, Paying in / Cheque Book stubs	Last completed Audit year	Audit
Insurance company names and policy numbers	Active + 6 years	Management, Limitation Act
Insurance Policies	Active + 3 years	Management, potential claims
Employer's Liability Certificates	40 years from commencement/renewal	Statute
Budgets	Indefinite	
Quotations and Tenders	6 Years	Limitations Act
Payroll records	12 years	Superannuation
Timesheets	4 years	Personal Injury
Recruitment Documents	Term of Employment + 6 years	Limitation Act
Documents on persons not hired	4 months post application process	Equal Opportunities Claims
Accident or Injury at work	7 years	Limitation Act

**MIDDLEWICH TOWN COUNCIL
DATA PROTECTION POLICY**



Personnel Administration (inc. CVs, appraisal disciplinary records, contracts, pay awards etc)	6 years after person leaves council except staff working with children (25 years)	Local choice and Statute
Personnel Service Record (Name, position, dates of employment, pay levels etc)	Term of Employment + 6 years	Limitation Act
Room Booking / Hire Records	3 years	Management
Folk and Boat Festival Records (Financial, Performance contracts, accounts)	6 years	Limitation Act, VAT
Details of Persons Purchasing events Tickets	Date of event + 6 months	Local choice, management. Payment queries