

Great Aycliffe Town Council



GENERAL DATA PROTECTION REGULATION POLICY

Author of Policy: Corporate and Policy Officer
Policy Effective from: October 2021
Revision Dates: January 2026



Contents

UK GENERAL DATA PROTECTION REGULATION 2018.....	1
DATA PROTECTION POLICY.....	1
Introduction	1
Aims of the Policy.....	1
Who Does this Policy Apply To?	1
Individual Responsibilities	1
Data Protection Principles	2
Data Protection and Data Security	2
Personal Data and Activities Covered by this Policy	3
Personal Data the Council Processes About Employees and Members	3
Sensitive Personal Data	4
How the Council Uses Personal Data	4
Accuracy and Relevance.....	4
Storage and Retention	5
Individual Rights	5
Data Security.....	6
Security Measures.....	6
Privacy Impact Assessments	6
Data Breaches	6
Training	7
Definitions	8
Data Protection laws	8
Personal Data	8
Sensitive or Special Categories of Data	8
Data Controller	8
Data Subject.....	8
Processing	8
Third Party.....	8
Relevant Filing System.....	8

UK GENERAL DATA PROTECTION REGULATION 2018

DATA PROTECTION POLICY

Introduction

- 1 Great Aycliffe Town Council is committed to ensuring that all personal data it handles will be processed according to legally compliant standards of data protection and data security.
- 2 It is confirmed for the purposes of the data protection laws, that the Town Council is a data controller of personal data in connection with employment or data needed for the services it provides, such as memberships. This means that the Council determines the purposes for which, and the manner in which, personal data is processed.
- 3 This policy should be viewed in conjunction with the Council's IT, Computer and Communications – Acceptable Use Policy, and the Social Media Policy.

Aims of the Policy

- 4 The purpose of this policy is to help the Town Council achieve its data protection and data security aims by:
 - Notifying employees of the types of personal information that the Council may hold about them, its customers, suppliers and third parties and what is done with that information.
 - Setting out the rules on data protection and the legal conditions that must be satisfied when the Council collects, receives, handles, processes, transfers and stores personal data and ensures staff understand the rules and legal standards.
 - Clarifying the responsibilities and duties of employees in respect of data protection and data security.

Who Does this Policy Apply To?

- 5 This policy applies to all Town Council employees and members.
- 6 Where data is required to be shared with third parties, a Data Sharing Agreement will be entered into.

Individual Responsibilities

- 7 Employees and members are responsible for helping to ensure the Town Council keep their personal data up to date.
- 8 Employees and Members should let the appropriate officer know when personal data provided to them changes e.g. if their bank details change.
- 9 Employees may have access to the personal data of other staff members and our customers in the course of their employment. Where this is the case, the Town Council relies on employees to help meet its data protection obligations.
- 10 Individuals who have access to personal data are required:
 - To access only personal data that they have authority to access and only for authorised purposes.

- Not to disclose personal data except to individuals, who have the appropriate authorisation.
- To keep personal data secure, by complying with rules on access to premises, computer access, including password protection and secure file storage and destruction.
- Not to remove personal data, or devices containing, or that can be used to access personal data, from the premises 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.

Data Protection Principles

11 Employees whose work involves using personal data relating to staff or others must comply with this policy and with the following Article 5 of the Data Protection Principles, which require that personal information is:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1)(*Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*), not be considered to be incompatible with the initial purposes ('purpose limitation').
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').
- 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 ('integrity and confidentiality').
- The Town Council, as data controller, shall be responsible for, and be able to demonstrate compliance with, the UK General Data Protection Regulation.

Data Protection and Data Security

12 Maintaining appropriate standards of data protection and data security is a collective task shared between the Town Council and employees and members as the data subjects. This policy and the rules contained in it apply to all employees of the Town

Council, irrespective of seniority, tenure and working hours. It also applies to members, consultants, contractors, casual or agency staff and trainees.

- 13 For further information, or questions about this policy, contact the Town Clerk.
- 14 All employees have personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that the measures are taken to protect data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. The Town Clerk must be notified if this policy has not been followed, or if it suspected that the policy has not been followed, as soon as reasonably practicable.
- 15 Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing staff or customer personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Personal Data and Activities Covered by this Policy

- 16 This policy covers personal data:
 - Which relates to a living individual who can be identified either from that information in isolation or by piecing it together with other information the Council possesses.
 - Is stored electronically or on paper in a filing system.
 - Which relates to staff (present, past or future) or to any other individual whose personal data the Council handles or controls.
 - Which the Council obtains, is provided with, holds or stores, organises, discloses or transfers, amends, retrieves, uses, handles, processes, transports or destroys.
- 17 The personal data is subject to the legal safeguards set out in the data protection laws.

Personal Data the Council Processes About Employees and Members

- 18 The Council collects personal data about employees which:
 - Employees provide or are gathered before or during employment or engagement with the Council.
 - Is provided by third parties, such as references or information from suppliers or another party that the Council does business with, or
 - Is in the public domain.
- 19 The types of personal data that the Council may collect, store and use about employees and members include records relating to their:
 - Home address, contact details and next of kin contact details.
 - Recruitment (including application form or curriculum vitae, references received and details of qualifications).
 - Pay records, national insurance number and details of taxes and any employment benefits such as pension details.
 - Telephone and email information.

- Performance and any disciplinary matters, grievances, complaints or concerns in which employees are involved.

Sensitive Personal Data

- 20 The Council may from time to time need to process sensitive personal information.
- 21 The Council will only process sensitive personal information if:
- There is a lawful basis for doing so, eg. it is necessary for the performance of the employment contract, and
 - One of the following special conditions for processing personal information applies:
 - The data subject has given explicit consent.
 - The processing is necessary for the purpose of exercising the employment law rights or obligations of the Town Council or the data subject.
 - Processing relates to personal data which are manifestly made public by the data subject.
 - The process is necessary for the establishment, exercise, or defence or legal claims, or
 - The processing is necessary for reasons of substantial public interest.
- 22 The Council's privacy notice sets out the type of sensitive personal information that are processed, what it is used for and the lawful basis for the processing.

How the Council Uses Personal Data

- 23 The Council will set out the reasons for processing personal data, how it uses such information and the legal basis for processing in its privacy notice. The Council will not process staff and members' personal information for any other reason.
- 24 In general, the Council will use information to carry out its business, to administer employment or engagement and to deal with any problems or concerns employees may have, including, but not limited to:
- **Employees' Address Lists:** to compile lists of home addresses and contact details to contact employees outside working hours or as part of an emergency response.
 - **Sickness Records:** to maintain a record of sickness absence and copies of any doctor's notes or other documents supplied in connection with employees' health, to manage absence to deal with unacceptably high or suspicious sickness absence, to monitor sickness absence across the Town Council.
 - **Disciplinary, grievance or HR matters:** in connection with any disciplinary, grievance or other HR related matters to ensure compliance with policies and procedures.
 - **Appraisals:** to enable appraisals to take place.

Accuracy and Relevance

- 25 The Council will:
- Ensure that any data is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.
 - Not process personal data obtained for one purpose for any other purpose, unless employees agree to this or reasonably expect this.

- 26 If employees consider that any information held about them is inaccurate or out of date then they should inform the applicable section within the Town Council immediately. If it is agreed the information is inaccurate or out of date, then it will be corrected promptly. If the relevant section does not agree with the correction, then the employee's comments will be noted.

Storage and Retention

- 27 Personal data (and sensitive personal information) will be kept securely in accordance with the Council's Document Retention and Disposal policy.
- 28 The periods for which the Council holds personal data are contained within the Document Retention and Disposal Policy.

Individual Rights

- 29 Anyone has the right to make a subject access request. If a subject access request is made, the Council will set out:
- What information is held on the data subject
 - For how long the personal data is stored.
 - The data subject's rights of rectification or erasure of data (right to be forgotten).
 - The right to complain to the Information Commissioner if the data subject thinks the Council has failed to comply with their data protection rights.
- 30 Anyone wishing to make a subject access request must contact the manager of the service it is believed has the information required, in writing. In case of uncertainty, please contact the Corporate & Policy Officer for assistance.
- 31 The Council will provide a copy of the personal data. This will normally be in electronic format, unless requested otherwise.
- 32 Proof of identification must be provided before a request can be processed. The Council will advise what documents are required.
- 33 The Council will normally respond to requests within 28 days of receipt. In complicated cases, or where additional time is needed, the Council will provide a response time frame.
- 34 If a request is manifestly unfounded or excessive, the Council is not obliged to comply with it.
- 35 Everyone has a number of other rights in relation to their personal data. Anyone can require the Council to:
- Rectify any inaccurate data.
 - Stop processing or erase data that is no longer necessary for the purpose of processing.
 - Stop processing or erase data if their interests override the Council's legitimate grounds for processing the data (where the Council relies on legitimate interests as a reason for processing data).
 - Stop processing data for a period if data is inaccurate or there is a dispute about whether or not the data subject's interests override the Town Council's legitimate grounds for processing the data.

Data Security

- 36 The Council will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 37 The Council will ensure that only the people who are authorised to use the information can access it.
- 38 The Council will ensure that personal data is accurate and suitable for the purpose for which it is processed.
- 39 The Council will use secure storage for any personal data using restricted access and passwords if required.
- 40 The Council will not transfer any data unless required to do so as part of an on-going management issue or in relation to wages and pensions or if required as part of a police investigation.

Security Measures

- 41 Any desk or cupboard containing confidential information must be kept locked.
- 42 Computers should be locked and shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
- 43 Personal data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- 44 All servers containing sensitive personal data must be protected by security software.
- 45 Particular care must be taken by employees who deal with telephone enquiries to avoid inappropriate disclosures such as personal information. Employees must not allow callers to bully them into disclosing information. Anyone who is being persistent or causing issues should be referred to a member of the senior management team.
- 46 Copies of personal information on paper must be shredded when no longer needed. Any electronic data should be deleted when no longer needed. Time frames for retention are set out in the Document Retention and Disposal Policy.
- 47 When computers and laptops are replaced they will be stored in the council offices until they can be securely disposed of.

Privacy Impact Assessments

- 48 When undertaking a project employees should consider if any personal data would be required. If so, a Privacy Impact Assessment (PIA) must be completed and, if appropriate, appended to the associated committee report. The PIA must be retained in the GDPR folder in the electronic filing system.

Data Breaches

- 49 If the Council discovers that there has been a breach of personal data that may pose a risk to the rights and freedoms of the individual, it will be reported to the Information Commissioner's Office within 72 hours of discovery and further advice will be sought.
- 50 The Council will record all data breaches, regardless of their effect, in accordance with the Data Breach Policy.
- 51 If the breach is likely to result in a high risk to the rights and freedoms of the individual, the Council will tell them that there has been a breach and provide them with more information about what has happened, any mitigation measures taken and the right to complain to the Information Commissioner's Office.

Training

- 52 The Council will provide training to all employees and members about their data protection responsibilities as part of the induction process, and whenever required after that.
- 53 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests will receive additional training, as applicable, to help them understand their duties and responsibilities and how to comply with them.

Definitions

Data Protection laws

All applicable laws relating to the processing of Personal Data.

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number and ID number. It also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive or Special Categories of Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions and biometric data. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data, disclosure or otherwise making available of data.

Third Party

Any individual/organisation other than the data subject, the data controller or its agents.

Relevant Filing System

Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic, CCTV etc. from which the individual's information can be readily extracted