Woodbridge TOWN COUNCIL

DATA PROTECTION POLICY

Woodbridge Town Council ('The Council') aims to ensure that personal information/data is treated lawfully and correctly.

The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the Council deals and in achieving its objectives.

This policy applies to all officers, Members and those engaged undertaking business with or on behalf of the Council.

The Council fully endorses and adheres to the Data Protection principles set out below: -

DATA PROTECTION PRINCIPLES

These principles are taken from the Information Commissioners Office website.

Personal Information shall be:

- Processed fairly, lawfully and in a transparent manner;
- Collected for specific, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to meet the purpose;
- Accurate and up to date;
- Kept for no longer than is necessary;
- Kept secure to maintain integrity and confidentiality;
- Processed in an accountable manner;

Policy Aim

To ensure the Council continuously complies with all relevant legislation and good practice in order to successfully protect the data it holds and processes.

Policy Objectives

To achieve the overall aim the Council will:

- Provide adequate resources to support an effective corporate approach to Data Protection;
- Ensure all staff are appropriately trained to perform their roles;
- Comply with all relevant statutory obligations;
- Respect the confidentiality of all personal data, irrespective of source;
- Publicise the Council's commitment to Data Protection;
- Compile and maintain appropriate policies, procedures and documentation;
- Promote general awareness and provide specific training, advice and guidance at all levels to ensure standards are met;
- Monitor and review compliance with legislation and introduce changes where necessary;
- Assist the Regulator and auditors as necessary

Processing of Information:

The Council, through appropriate management controls will, when processing personal information on any individual:

- Observe fully conditions regarding the collection and use of information to meet the Council's legal obligations under Data Protection legislation;
- Collect, process and retain data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement;
- Ensure that the rights of people about whom information is held can be fully exercised including: -
    - The right to be informed that processing is being undertaken;
    - The right of access to personal information;
    - The right to withdraw or amend consent for processing*;

  - The right to correct, amend or erase information*;
  - The right to be forgotten*.

- Ensure staff are reminded that data covered by Data Protection legislation is exempt from disclosure under the Freedom of Information Act 2000.
- *Ensure where an individual exercises their right to be forgotten or withdraws permission for their data to be processed, the Council will inform the subject of the potential impact of this decision, as it may prevent the Council being able to provide a service which the subject has requested.
- Note: The right to be forgotten or withdraw permission for processing does not apply where the Council has a statutory obligation or requirement to process that information.

Fair Obtaining/Processing

Individuals whose data is collected by the Council must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of an individual's data can take place unless reasonable steps have been taken to make that individual aware of that processing.

Individuals must also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information (Data Protection Officer).

When consent is used as the lawful basis for processing data, it must be explicit and granular to allow the subject to 'opt-in' to any processing activity. The Privacy Notice where this data is collected should also explain how a subject's data will be used, how they can amend or withdraw their consent, and whom they should contact to do so.

Data Uses and Purposes

- All processing performed must only be for the purpose that is necessary to enable the Council to perform its duties and services, and which has been notified by the Council to the Information Commissioner. Personal data can only be processed in line with notified purposes.
- No new processing may take place unless the data subjects have been informed, and their consent obtained.

- All personal data should be regarded as confidential and only disclosed to persons (internal and external) who are listed for the purpose concerned in the Council's current notification AND whose authority to receive it has been explicitly established.
- Information owned by the Council must not be used for non-Council purposes. This applies when Council data is being processed at employees' homes. Employees will be held responsible for any misuse or unauthorised disclosures while the data is in their control.

What counts as Personal Data?

The term ‘ ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The regulations apply to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the regulations depending on how difficult it is to attribute the pseudonym to a particular individual. Likewise, anonymised data that can be ‘reverse engineered’, or manipulated on its own or in conjunction with other data sources to identify an individual, will also be classified as personal data.

A name and address, or information attached to a reference number that we can use to look someone up, are both personal data. So is a company e-mail address if it includes a person’s name.

Data Quality & Document Retention

Information processed shall not be excessive or irrelevant to the notified purposes.

Information will be held only for as long as is necessary for the notified purposes, after which it shall be deleted or destroyed in accordance with the Council’s Document

Retention periods.

Whenever information is processed, reasonable measures shall be taken to ensure that it is up-to-date and accurate. A data subject has the right to request that any errors or omissions are rectified.

Organisational Responsibilities and Security

All personal data should be kept secure, in a manner appropriate to its sensitivity and the likely harm should a breach occur. Security shall be applied to all stages of processing to prevent unauthorised access or disclosure (internal or external), damage (accidental or deliberate) or loss.

Personal data must not be left on display or unsecured when unattended. Computer software shall be kept secure when not in use. System entry passwords should be known only to the holder and be changed regularly.

Everyone managing and handling personal information must be appropriately trained to do so.

Everyone managing and handling personal information must be appropriately supervised.

Anybody wanting to make enquiries about handling personal information must know how to do so.

Queries about handling personal information must be promptly and courteously dealt with.

Methods of handling personal information must be clearly described.

An annual review and audit shall be made of the way personal information is managed.

Methods of handling personal information shall be assessed and evaluated on an on-going basis by the Data Controller.

Performance with handling personal information shall be assessed and evaluated on an on-going basis by the Data Controller.

All Council employees and Members shall be provided with a copy of the Policy as adopted by the Council, together with appropriate training. All new councillors shall be offered training in the principles of Data Protection and how to avoid being tricked into revealing personal data.

Training shall be re-offered at the start of every 4-year council term, and councillors will be asked to formally acknowledge that it has been offered.

Employees have a duty to follow the Policy and procedures and to co-operate with the Council to ensure this Policy is effective.

Action may be taken against any employee/Member who fails to comply or commits breach of the Policy.

It is the duty of individual employees and Members to ensure that personal information held by them is dealt with in accordance with Data Protection legislation.

Processing carried out by a third party on behalf of the Council shall be subject to a contract, which stipulates compliance with Data Protection regulations and this policy.

Similarly, when the Council is processing personal data on behalf of a third party it will need to demonstrate that the data is subject to the same standards of care.

Breach of protocol

A personal data breach is defined on the ICO website as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service." It may be deliberate or accidental.

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the Officer or Councillor must inform the Town Clerk and DPO immediately in order that an assessment can be made as to whether the ICO should be informed within 72 hours as is legally required, and / or those data subjects affected by the breach. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

The procedures laid out by the ICO on their website (see below), will be followed in the event of a data breach:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Complaints & Queries

Queries regarding this policy should be addressed to the Data Protection Officer which is the Town Clerk at townclerk@woodbridge-suffolk.gov.uk

If you are not happy with the Council's response to a Data Protection request, you can complain using the Council's complaints procedure (TCP 5 on the Council's website)

You can speak to your local Councillor(s) to see if they can resolve the issue for you.
If you are unclear who this is, telephone the Council Officers (01394 383599) or visit our

website (www.woodbridge-suffolk.gov.uk).

You can complain to the Information Commissioner at:
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545 700

Web: www.ico.gov.uk

Approved – 20.09.23
Review – Annually.