DATA PROTECTION POLICY

This policy provides internal guidance relating to the collection and processing of personal data held by the Council, falling within the scope of the GDPR and the Data Protection Act 2018, in all formats including paper, electronic, audio and visual.

The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes personal data. This includes staff members, meaning employees, agency staff and those retained on a temporary or permanent basis, and Councillors.

Where a Councillor is also deemed to be a Data Controller in their own right, they may be required to register with the Information Commissioner's Office (ICO) and pay the relevant fee. Members should visit the ICO website (www.ico.org.uk) for more information.

Separately, the Council's 'General Data Privacy Notice' and 'Data Privacy Notice for Staff & Councillors' provides information for any individual for whom the council processes personal data.

Introduction

Woodley Town Council ("the Council") is fully committed to compliance with the requirements of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (the DPA). The Council will, therefore, follow procedures which aim to ensure that all personal data collected about Councillors, staff, visitors and other individuals is processed fairly, lawfully and transparently.

The GDPR, the DPA and Article 8 of the Human Rights Act 1998, stress that the processing of personal data needs to strike a balance between the needs of the Council to function effectively and efficiently and respect for the rights and freedoms of the individual. This policy sets out how the Council intends to safeguard those rights and freedoms.

The Council will follow procedures that aim to ensure that all Councillors, staff, visitors and any other person working for the Council who have access to any personal data held by or on behalf of the Council is fully aware of, and abides by their duties and responsibilities under the General Data Protection Regulation and Data Protection Act.

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken.

As well as the Council, any individual who knowingly or recklessly processes data without appropriate consent or proper authorisation, for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to the Council's disciplinary procedures, including dismissal where appropriate, and possible legal action liable to prosecution and possible criminal conviction under the Criminal Justice and Immigration Act 2008.

Personal and special category personal data

The GDPR and DPA provides conditions for the collection and processing of any personal data. It also makes a distinction between 'personal data' and 'special category personal data'.

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.

Special category 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 or sexual orientation;
- genetics
- biometric data (where used for ID purposes)

Special category data includes personal data revealing or concerning the above types of data. Therefore, if data may allow you to infer details about someone which fall into one of the above categories, it may count as special category data.

Although there are clear distinctions between personal and special category data for the purposes of this policy the term 'personal data' refers equally to 'special category personal data' unless otherwise stated.

The GDPR and DPA rules for special category data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

Personal data processed by the Council

The Council processes personal data for a variety of Council purposes about our employees, residents, suppliers and other individuals. A description of the types of personal data processed and the purposes for processing are covered in the Council's privacy notices and 'Personal Data Audit' document.

Personal data must be handled and dealt with in accordance with the GDPR and DPA, this policy, and the Council's privacy notices, 'Personal Data Audit' and Information Security Policy.

The Data Controller

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed. Woodley Town Council is the Data Controller for all personal data relating to its Councillors, employees, residents, suppliers and any other individuals.

Roles and Responsibilities

Town Clerk

The Town Clerk has overall responsibility for ensuring that the Council complies with all relevant data protection obligations and acts as the respresentative of the data controller on a day-to-day basis.

Data Protection Officer

The Council is not required to employ a Data Protection Officer (DPO) and the Town Clerk will maintain responsibility for overseeing the implementation of this policy, monitoring the compliance with data protection law, and developing related policies and guidelines where applicable.

They can be contacted via email at: townclerk@woodley.gov.uk

Staff and Councillors

All staff and Councillors are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy, the Council's data privacy notices, 'Personal Data Audit' and Information Security Policy;
- Informing the Council of any changes to their personal data, such as a change of address;
- Contacting the Town Clerk if you:
  - Have questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
  - Have concerns that this policy is not being followed;
  - Are unsure whether or not you have a lawful basis to use personal data in a particular way;
  - Need to rely on or capture consent, deal with the rights of the data subjects or transfer personal data outside the European Economic Area;
  - Believe there has been a data breach;
  - Are engaging in a new activity that may affect the privacy rights of individuals;
  - Need help with any contracts or sharing personal data with third parties.

Data Protection Principles

Anyone processing personal data must comply with the principles of good practice. These principles are legally enforceable and can be summarised as follows:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Obtained 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 not be considered to be incompatible with the initial purposes;
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;
5. 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. 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. In accordance with the rights of data subjects under the GDPR and DPA.

Fair Processing
In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as is necessary to ensure that they are likely to understand:

a) The purposes for which their personal data are to be processed;
b) The likely consequences of such processing and;
c) Whether particular disclosures can be reasonably envisaged

Notification
The national body for the supervision of GDPR is the Information Commissioners' Office to whom the Town Clerk notifies their purposes for processing personal data.

This notification process serves to provide transparency and openness about the processing of personal data. It is a fundamental principle of the GDPR that the public should know or be able to find out who is carrying out the processing of personal data and for what purpose.

A copy of the Council's notification details is available on the Information Commissioner's website www.ico.org.uk. The Council's ICO registration number is Z4915658.

Individuals' Rights
The Council recognises that access to personal data held about an individual is a fundamental right provided in the Act. These rights include:

- The right to be informed
- The right of access to personal information
- The right to request rectification
- The right to request erasure
- The right to restrict processing in certain circumstances
- The right to data portability
- The right to object to processing
- Rights related to automated decision-making including profiling

The Council will ensure that all requests from individuals to access their information is responded to within one calendar month which is the time allowed in the legislation. However, the one-month timescale will not commence until after receipt of all identity is received.

Where possible, and to speed up processing, requests should be made in writing via email to townclerk@woodley.gov.uk. However, requests may also be received in writing via post, on social media, or verbally. All requests will be treated equally.

To minimise delays and unnecessary work all requests from data subjects should:

- Be accompanied by adequate proof of identity of the data subject to allow us to confirm their identity;
- Provide written authorisation of the data subject where the request is being made by someone else on their behalf (e,g. a friend, relative, legal representative);
- Specify clearly and simply the information being sought;
- Give adequate information to enable the requested data to be located;
- Make it clear where the response should be sent.

The Town Clerk must be informed of any request to action against one or more of these rights.

The Act allows exemptions from providing information to individuals making a subject access request, and non-disclosure of information, in specific and limited circumstances.

When the Council collects personal data the Council does not need to provide the individual with any information they may already have.

When obtaining personal data from other sources, the Council do not need to provide individuals with privacy information if:

- The individual already has the information;
- Providing the information to the individual would be impossible;
- Providing the information to the individual would involve disproportionate effort;
- Providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- The Council is required by law to obtain or disclose the personal data; or
- The Council is subject to an obligation of professional secrecy regulated by law that covers personal data

If a data subject remains dissatisfied with a response received, they may ask for the matter to be reviewed, or in the case of an employee a resolution may be sought using the Council's grievance process.

Ultimately, if a data subject continues to be dissatisfied, they have the right to ask the Information Commissioner's Office (ICO) to carry out an assessment of their case and pursue a legal remedy if appropriate.

Legal Requirements

The Council may be required to disclose personal data by a court order, or to comply with other legal requirements including the prevention or detection of crime, apprehension of an offender or gathering of taxation.

External agencies or companies contracted to undertake processing of personal data on behalf of the Council must demonstrate, via a written agreement, that personal information belonging to the Council will be handled in compliance with the GDPR and DPA and that it has the necessary technical and organisational security measures in place to ensure this.

Any sharing of the Council data with external partners for the purpose of service provision must comply with all statutory requirements.

The Council will follow relevant guidance issued by the Government and the ICO for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and employees have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same. The Council reserves the right to monitor telephone calls, email and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO.

The legal basis for this policy is the GDPR and DPA which provides the legal parameters for the processing of personal data. However, compliance with other legislation, Codes of Practice, policies and guidance also has relevance, such as:

- The Freedom of Information Act 2000
- The Computer Misuse Ace 1990
- The Crime and Disorder Act 1998
- Human Rights Act 1998

Data Security - General
To ensure the security of personal data, the Council has appropriate physical, technical and organisational measures in place. All staff must comply with the terms and conditions of their employment, including complying with the Council's Information Security Policy.

The GDPR and DPA requires that appropriate technical and organisational measures shall be taken to protect data against:

- Unauthorised access;
- Unauthorised or unlawful processing;
- Accidental loss, destruction, or damage.

Appropriate technical and organisational security measures will include:

- Using and developing technological solutions to ensure compliance with the data protection principles;
- Using and developing physical measures to protect Town Council assets;
- Ensuring the reliability of any persons who have access to Town Council information;
- Reporting and investigating security breaches.

These obligations include the need to consider the nature of the data to be protected and the harm that might arise from such unauthorised or unlawful processing or accidental loss, destruction, or damage.

In general, the Council will only keep data for as long as it is needed. The Council may have legal obligations to retain some data in connection with our statutory obligations as a public authority. Some records will be kept permanently where we are legally required to do so, whilst other records may be kept for an extended period of time; for example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information.

Once data is no longer needed, it must be deleted or anonymised. Details of the length of time types of data are kept, and the individual staff members responsible for the retention and deletion of the data, is included in the Council's 'Personal Data Audit' document.

All hard copy documentation (i.e. printout material, manual files, hand written notes etc) which contain personal data and are no longer required must be treated as confidential waste and disposed of securely.

Where processing of Council data is to be carried out by a third party on behalf of the Council, the Town Clerk must ensure that the third party provides sufficient guarantees in respect of the technical and organisation measures governing the processing to be undertaken, including the signing of an appropriate Data Sharing Agreement.

Data Security – Specific
The following specific processes must be followed in relation to processing personal data:

- When processing card payments, staff must comply with the Council's Information Security Policy; this includes not writing down or storing cardholder data, nor repeating data so as to ensure they cannot be overheard;
- Where, with prior agreement from their Manager, individuals access, create or store Council work on a personal device, the device must be secured (password protected or equivalent), and the work transferred to a Council owned device and deleted from the personal device as soon as possible; this is particularly important if the work contains information which may include personal data.
- Email communication between Officers and Councillors regarding Council business should only take place via the official Town Council email system (i.e. @woodley.gov.uk email addresses). Emails received on a Town Council email address should not be sent or forwarded to an alternative, personal email address where any data included is, or might contain confidential or personal data. This is to ensure the security of confidential and / or personal data being circulated between staff and Councillors.

Further details on information security and the safe use of IT are included in the Council's Information Security Policy.

Sharing Personal Data

The Council will not normally share personal data with anyone else, but may do so where:

- There is an issue that puts the safety of our staff at risk;
- The Council need to liaise with other agencies – the Council will seek consent as necessary before doing this;
- Our suppliers or contractors need data to enable the Council to provide services to staff and residents, for example, IT companies. When doing this, the Council will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the Council share;
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Council.

The Council will also share personal data with law enforcement and government bodies where the Council are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

The Council may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our staff or Councillors.

Where the Council transfer personal data to a country or territory outside the European Economic Area, the Council will do so in accordance with data protection law.

CCTV
Where the Council uses CCTV the Council will adhere to the ICO's code of practice for the use of CCTV. The Council do not need to ask individuals' permission to use CCTV, but will make it clear where individuals are being recorded, with cameras clearly visible and accompanied by prominent signs explaining that CCTV is in use. Officers involved in the management or conducting of CCTV will be required to follow the Council's separate CCTC Policy.

Personal data breaches
The Council will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the Town Clerk must be notified immediately. Data breaches will be tracked on the Council's 'Data Breach Incident Log'.

Where the breach is likely to result in a high risk to individuals' rights and freedoms, those impacted must be informed directly without undue delay.

When appropriate, the Council will report the data breach to the ICO within 72 hours. Such breaches in a Town Council context may include, but are not limited to:

- The theft of a Council or personal electronic device containing non-encrypted personal data about staff, Councillor and / or members of the public;
- Accidental disclosure of personal data to another person or organisation;
- Inappropriate access to or use of personal data;
- The theft of personal information, either paper based or electronic;
- Accidental loss of personal data;
- Information that has not arrived at its destination;
- Fraudulent acquisition of personal data.

Training and awareness
Data Protection training and awareness is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the GDPR and DPA can result in significant fines or criminal prosecution.

It is the Council's policy that all staff must complete appropriate GDPR training annually. The Council will ensure that staff without IT access can also complete the appropriate training. Councillors are also expected to undertake this training.

Town Council commitment to data protection
The Town Clerk will be accountable for ensuring compliance with this policy.

The Council will ensure that individuals handling personal information will be trained to an appropriate level in the use and control of personal data.

The Council have implemented a process to ensure all individuals handling personal information know when and how to report any actual or suspected data breach(es), and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

The Council will monitor and review its processing activities to ensure these are consistent with the principles of the GDPR and DPA and will ensure that its notification is kept up to date.

The Council will ensure that any new or altered processing identifies and assesses the impact on a data subject's privacy as a result of any processing of their personal data, and that appropriate

Privacy Notices are maintained to inform data subjects as to how their data will be used.
The Council will review and supplement this policy to ensure it remains consistent with the Law and any compliance advice and Codes of Practice issued from time to time by the ICO.

Policy Review
The Town Clerk is accountable for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

This Policy was last reviewed in September 2023.