



## **Watton Town Council**

### **Privacy Notice (Employees)**

**June 2024**

---

#### **What is the purpose of this document?**

Watton Town Council is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation ("**UK GDPR**").

This privacy notice applies to all councillors, officers, employees, workers and contractors of Watton Town Council ("**WTC**", "**we**", "**us**", "**our**").

WTC is a "**controller**" as your employer. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation (including the UK GDPR) to notify you of the information contained in this privacy notice.

This notice applies to current and former councillors, officers, employees, workers and contractors of WTC. This notice does not form part of any contract of employment, other contract to provide services, or any contractual appointment as a councillor. We may update this notice at any time, but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information, and what your rights are under the UK GDPR and other applicable data protection legislation.

## Data protection principles

We will comply with data protection legislation. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

## The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (**anonymous data**).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation. Information about criminal convictions also warrants this higher level of protection.

Depending on your role, we will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date, and if different, the date of your continuous employment.
- Any leaving date and the reason for leaving.
- Location of employment or workplace.
- Copy of driving licence and online DVLA checks.
- Hours of work and attendance at work information.
- Information regarding periods of leave taken, including holiday, sickness absence, family leave and sabbaticals, and any leave from placement on the Coronavirus Job Retention Scheme, and the reasons for leave.
- Details of qualifications, skills, experience and employment history, including start and end dates with previous employers.
- Recruitment information (including copies of right to work documentation, passport, nationality information, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Terms and conditions of your employment.

Due for review June 2026

pg. 2 250624

- Remuneration history.
- Performance information (including appraisals, performance reviews and improvement plans).
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means.
- Information about your use of our information and communications systems.
- Information about your location, including location data.
- Photographs – we will only collect such data from you where we have received your consent to collect such data. Where we ask for such consent, this will be for explicit reasons, which we will confirm to you when gaining your consent.
- Results of any HMRC employment status check, details of your interest in and connection with the intermediary through which your service(s) are supplied.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records, including:
  - where you leave employment and the reason for leaving is determined to be ill-health, injury or disability, the records relating to that decision;
  - details of any absences (other than holidays) from work, including time on statutory parental leave, sick pay, or any time on the Coronavirus Job Retention Scheme (commonly referred to as the "Furlough Scheme");
  - any health information in relation to a claim made under health insurance scheme operated by WTC from time to time;
  - where you leave employment and the reason for leaving is related to your health, information about any relevant condition needed for pensions, or any health insurance purposes.
- Genetic information and biometric data.
- Information about criminal convictions and offences.

### **How is your personal information collected?**

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider or from a general online search. We may sometimes collect additional information from third parties including former employers, credit reference agencies, occupational health providers, online DBS checking service, online DVLA driving licence checking service or other background check agencies.

We may also collect information from the trustees or managers of any pension arrangements operated by us.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

### CCTV

We currently use CCTV around our site, as outlined below. We believe that such use is necessary for legitimate business purposes, including:

- a) to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- b) for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;

Due for review June 2026

pg. 3 250624

- c) to support law enforcement bodies in the prevention, detection and prosecution of crime;
- d) to assist in day-to-day management, including ensuring the health and safety of staff and others;
- e) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and
- f) to assist in the defence of any civil litigation, including employment tribunal proceedings.

This list is not exhaustive and other purposes may be or become relevant.

CCTV monitors the exterior of the building, along with the entrances of, and specific areas requiring security within, the building, 24 hours a day and this data is continuously recorded. Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purposes of monitoring, and as far as practically possible, CCTV cameras will not focus on private locations or property.

Images may be monitored by authorised personnel 24 hours a day, every day of the year. Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

Where CCTV cameras are placed in the workplace, we will ensure that signs are displayed at the entrance to surveillance zones to alert individuals that their image may be recorded.

Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety. We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved in disciplinary or grievance matters. Recorded images will only be viewed in designated, secure offices.

In order to ensure that the rights of individuals recorded by the CCTV system are protected we will ensure that data gathered from CCTV cameras is stored in a way that maintains integrity and security. This may include encrypting the data, where it is possible to do so. We may also store video footage using a cloud computing system, and will take all reasonable steps to ensure that any cloud service provider maintains the security and integrity of the data. Where we engage data processors to process data on our behalf, we will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

Data recorded by the CCTV system will be stored digitally using a cloud computing system. Data from CCTV cameras will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. We will maintain a comprehensive log of when data is deleted. At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

## How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract, we have entered into with you (for example, your employment contract).
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
4. Where we have obtained your consent to use your personal information.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

### Situations in which we will use your personal information

We need all the categories of information in the list above (see the heading entitled "**Error! Reference source not found.**") primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Determining whether your engagement is deemed employment for the purposes of Chapter 10 of Part 2 of the Income Tax (Earnings and Pensions) Act 2003 ("**ITEPA 2003**") and providing you with a status determination statement in accordance with applicable provisions of ITEPA 2003.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing other employment benefits to you.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and remuneration.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Plan for career development and succession planning.
- Gathering evidence and conducting possible grievance or disciplinary hearings/processes.
- Making decisions about your continued employment or engagement.

Due for review June 2026

pg. 5 250624

- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Promoting the business and marketing, including using your details on promotional materials and our website.
- Assessing whether your motor insurance covers business travel.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work and to comply with our duties in relation to individuals with disabilities
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- To manage and monitor all types of leave (including maternity, paternity, adoption, parental and shared parental leave, and any leave under the Coronavirus Job Retention Scheme).
- To provide references to prospective employers.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

### **If you fail to provide personal information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

### **Change of purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## How we use particularly sensitive personal information

**"Special categories"** of particularly sensitive personal information require higher levels of protection, such as information about your race, ethnicity, sexuality, political views or medical records. We need to have further justification for collecting, storing and using this type of personal information, and have in place appropriate safeguards which we are required by law to maintain and abide by when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with your employment, and do so in line with our Data Protection Policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Data Protection Policy.
4. Where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

## Our obligations as an employer

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with your employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will use your particularly sensitive personal information are listed below:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits, including statutory maternity pay, statutory sick pay, pensions, and any health insurance scheme we may operate from time to time. We need to process this information to exercise rights and perform obligations in connection with your employment.
- If you leave employment, and the reason for leaving is determined to be ill-health, injury or disability, we will use the information about your physical or mental health, or disability status in reaching a decision about your entitlements under any benefits provided by virtue of your employment (for example, any health insurance scheme we operate from time to time, or any ill-health pension which may be available under a pension arrangement operated by us from time to time).
- If we reasonably believe that you or another person are at risk of harm, and the processing is necessary to protect you or them from physical, mental or emotional harm, or to protect physical, mental or emotional well-being.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

## Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, or are at risk of harm and are unable to protect yourself.

## Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Data Protection Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we may hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

## Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you one month to request a reconsideration.
2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Due for review June 2026

pg. 8 250624



## Data sharing

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the United Kingdom.

If we do, you can expect a similar degree of protection in respect of your personal information.

### **Who has access to my data within Watton Town Council?**

We may share your personal information internally, including with members of the HR and recruitment team, your line manager and managers in the business area in which you work if access to the information is necessary for performance of their roles.

### **Why might you share my personal information with third parties?**

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. For example, we may share your information with third parties in order to obtain pre-employment references from previous employers, obtain medical information from occupational health providers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

### **Which third-party service providers process my personal information?**

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: Payroll, Pension Administration, Benefits Administration, legal advice, accountancy and IT Services.

We will also share personal data regarding your participation in any pension arrangement operated by us or any group entity with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements from time to time.

### **How secure is my information with third-party service providers?**

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### **What about other third parties?**

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction. We may also need to share your personal information with a regulator or to otherwise comply with our legal obligations. This may include making disclosures to HMRC or regulators, and disclosures to shareholders such as directors' remuneration reporting requirements.

## **Transferring information outside the UK**

We may transfer information we collect about you outside of the UK in order to perform our contract with you. Where we do so, we will ensure that there are adequacy regulations in respect of the country where data is being received, or other protective measures such as appropriate safeguards, binding corporate rules, or standard contractual clauses are in place. This means that your personal information will be treated by those third party recipients in the recipient country in a way that is consistent with and which respect UK law on data protection. Further information on these protective measures is available from the Data Compliance Manager.

## **Data security**

We have put in place measures to protect the security of your information. Details of these measures are available upon request from our Data Compliance Manager. Details of the Data Compliance Manager can be found in our Data Protection Policy.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those councillors, officers, employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## **Data retention**

### **How long will you use my information for?**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Data Retention Policy, and Register of Retention Periods.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the Council, we will retain and securely destroy your personal information in accordance with our data retention register.

## **Rights of access, correction, erasure, and restriction**

### **Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

### **Your rights in connection with personal information**

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact HR or the Data Compliance Manager in writing.

### **No fee usually required**

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

### **What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### **Right to withdraw consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact HR.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

### **Data Compliance Manager**

We have appointed a Data Compliance Manager to oversee compliance with this privacy notice and our other data protection compliance requirements. If you have any questions about this privacy notice, or how we handle your personal information, please contact the Data Compliance Manager. You have a right to make a complaint at any time to the Information Commissioner's Office (ICO) with respect to data protection issues.

### **Changes to this privacy notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.