

WWU Job Applicant Privacy Notice

CONTENTS

1. About this notice.....	3
2. How we collect your information	3
3. What information we may hold about you	4
4. Why we use your information	5
5. Our lawful basis for using your information	6
6. Special category information	7
7. Criminal offence information and vetting.....	7
8. Pre-employment checks	8
9. Who we share your information with.....	8
10. International transfers	9
11. Automated decision-making and AI	9
12. How we protect your information	10
13. How long we keep your information.....	10
14. If you do not provide information	11
15. Your rights.....	11
16. Keeping your information accurate	11
17. Questions, concerns and complaints.....	12
18. Changes to this notice.....	12

RECRUITMENT INFORMATION AT A GLANCE

Who is responsible for your information?

Wales & West Utilities Limited (WWU) is the data controller for information used during recruitment.

What information do we collect?

Depending on the role and recruitment stage, this may include application details, qualifications, work history, right to work status, pre-employment checks and, where relevant, occupational health, vetting and screening information.

Why do we collect it?

To assess applications, manage recruitment, complete appropriate checks, meet legal obligations and support onboarding if you are successful.

Who do we share it with?

Where necessary and lawful, we may share information with recruitment partners, screening providers, occupational health providers, regulators and other relevant organisations.

How long do we keep it?

Unsuccessful applicant records are usually retained for one year after the recruitment ends. Other records are retained in line with WWU retention rules.

Your rights

You have rights to access, correct, restrict, erase or object to the use of your information, depending on the circumstances.

Questions?

Contact the Data Protection Officer at dataprotection@wwutilities.co.uk

1. ABOUT THIS NOTICE

Wales & West Utilities Limited (“WWU”, “we”, “us” or “our”) is the data controller for personal information used during our recruitment process.

This notice explains how we collect, use, share, store and protect personal information about people who apply to work with us. This includes applicants for permanent, temporary, fixed-term, apprenticeship, contractor and agency roles where WWU is involved in the recruitment or selection process.

This notice applies during the recruitment process. If you are successful, some information collected during recruitment will become part of your employment record and will then be handled in line with our Employee Privacy Notice.

This notice does not form part of any contract of employment or contract to provide services.

To exercise any of your data protection rights, please contact our Data Protection Officer using the details set out in section 17 of this notice. We may ask for additional information to verify your identity before responding to a request.

2. HOW WE COLLECT YOUR INFORMATION

We collect most recruitment information directly from you. This may be through application forms, CVs, covering letters, interviews, assessments, correspondence, identity documents, right to work documents and information you provide during onboarding.

You may apply for roles through our website, recruitment partners, recruitment agencies, job boards, or other recruitment platforms we use from time to time. Where you apply through a third-party platform, that organisation may also be a controller of your personal information for its own purposes. You should read the privacy information provided by that platform.

We may also receive information from other sources where this is relevant to your application or required for pre-employment checks. These may include:

- recruitment agencies or other recruitment partners;
- referees and former employers;
- professional bodies, regulators, licensing bodies or certification organisations;
- education or training providers;
- background screening providers;
- Disclosure and Barring Service checks, where relevant and permitted by law;
- government departments or authorised vetting organisations, where security clearance or national security vetting is required;
- occupational health providers and testing providers;
- publicly available sources, but only where relevant, proportionate and appropriate for the role.

Where we receive information about you from another source, we will handle it in line with this notice and will provide further privacy information where required.

We will usually only seek references, background checks, occupational health checks, criminal record checks or vetting information once we are considering making, or have made, an offer of employment. Some checks will only apply to specific roles.

3. WHAT INFORMATION WE MAY HOLD ABOUT YOU

The information we use will depend on the role, the stage of the recruitment process and any legal, regulatory, safety or operational requirements that apply.

We may collect and use the following types of information.

Identity and contact information

This may include your name, address, telephone number, email address, date of birth, title, previous names, signature, and information from identity documents such as passports, driving licences or other proof of identity.

Application and recruitment information

This may include your CV, application form, covering letter, work history, qualifications, skills, professional experience, interview notes, assessment outcomes, test results and any correspondence with you about the role.

Professional, regulatory and competency information

For some roles, we may need information about professional registrations, licences, qualifications, certifications, competency schemes, Gas Safe registration details, security-related declarations or other role-specific requirements.

Right to work and onboarding information

This may include evidence of your entitlement to work in the UK, nationality or immigration information, passport or visa details, National Insurance number, bank details, tax information, emergency contact details (where collected after offer or during onboarding) and information needed to set up employment, payroll, pensions, benefits and system access if you are successful.

Occupational health and fitness for work information

Where relevant to the role or recruitment process, we may process occupational health information, fitness for work information, workplace adjustment information, pre-placement assessment information, health declaration information, drug and alcohol testing information and summary certificates or outcomes provided by occupational health providers.

We will only use occupational health information where it is necessary and access will be limited. We will not routinely share detailed medical reports with hiring managers. Where information needs to be shared internally, this will normally be limited to fitness for work outcomes, restrictions, adjustments, recommendations, test outcomes or information necessary to support a safe and fair recruitment decision.

Where an occupational health provider is involved, WWU will normally receive information necessary to make a recruitment, fitness for work, safety or workplace adjustment decision unless additional information is necessary for the stated purpose and permitted by law. We do not routinely receive full clinical records.

Equality, diversity and inclusion information

We do not currently collect equality monitoring information as part of the application process. If this changes in future, we may collect information such as ethnicity, disability, sex, sexual orientation, religion or belief, or other diversity information to help us monitor and improve the fairness and inclusivity of our recruitment processes. If equality monitoring information is collected, participation will normally be voluntary unless otherwise specified. Any such information would not be used to make recruitment decisions and, where possible, would be reported in anonymised or aggregated form.

You are not required to provide equality monitoring information unless we tell you otherwise. If you choose not to provide it, this will not affect your application.

Criminal offence, security screening and vetting information

For some roles, we may need information relating to criminal convictions, criminal offences, security screening or national security vetting. This will only be requested where relevant to the role and where WWU is legally permitted or required to carry out the check.

For example, some roles may involve access to critical national infrastructure, regulated environments, restricted systems, safety-critical work, sensitive information or positions of trust. In those cases, we may need to carry out additional checks before confirming employment.

4. WHY WE USE YOUR INFORMATION

We use applicant information to manage recruitment fairly, safely and lawfully. This includes:

- receiving and managing applications;
- assessing your skills, qualifications, experience and suitability for a role;
- communicating with you about your application;
- arranging interviews, assessments and tests;
- making recruitment decisions;
- verifying information you have provided;
- checking your right to work in the UK;
- obtaining references and carrying out pre-employment checks;
- assessing fitness for work and any adjustments needed;
- meeting health, safety, regulatory, security and employment obligations;
- managing role-specific checks, such as professional registrations, competency requirements or security vetting;
- creating employment, payroll, pension, benefit and system access records if you are successful;
- keeping appropriate recruitment records;
- responding to complaints, queries, audits, investigations or legal claims;
- monitoring and improving the fairness, effectiveness and governance of our recruitment process.

We will not use your information for purposes that are incompatible with your application unless we have a lawful basis to do so and, where required, we provide further privacy information.

Our legitimate interests include recruiting suitable people, running a fair and effective recruitment process, protecting our business, meeting security and safety requirements, and responding to complaints or legal claims.

5. OUR LAWFUL BASIS FOR USING YOUR INFORMATION

We must have a lawful basis under UK data protection law before using your personal information. More than one lawful basis may apply depending on the purpose and stage of recruitment.

Purpose	Types of information	Lawful basis
Managing your application and assessing your suitability	Identity, contact, application, recruitment, interview and assessment information	Legitimate interests, to recruit effectively and select suitable candidates. Pre-contractual steps, where processing is needed before entering into an employment contract
Communicating with you about recruitment	Identity and contact information	Legitimate interests. Pre-contractual steps
Checking right to work in the UK	Identity, nationality, immigration and right to work information	Legal obligation. Pre-contractual steps
Verifying qualifications, licences, professional registrations and competency requirements	Identity, recruitment, professional and compliance information	Legitimate interests. Legal obligation where checks are required by law or regulation
Pre-employment checks, references and background screening	Identity, contact, recruitment, employment history, reference and screening information	Legitimate interests. Legal obligation where checks are required. Pre-contractual steps
Occupational health, fitness for work, drug and alcohol testing and workplace adjustments	Health, occupational health, testing and adjustment information	Legal obligation and/or legitimate interests, depending on the role and context. Special category conditions are explained below
Security screening, criminal record checks and national security vetting	Identity, address history, vetting, criminal offence and security screening information	Legal obligation and/or legitimate interests, depending on the role and requirement. Criminal offence information is handled under the Data Protection Act 2018 safeguards
Equality monitoring and recruitment reporting (where collected)	Equality and diversity information	Legitimate interests in monitoring and improving recruitment fairness. Where this involves special category information, the relevant conditions are explained below.
Creating employment records if you are successful	Identity, contact, onboarding, payroll, pension, tax, benefit and system access information	Contract. Legal obligation. Legitimate interests
Handling complaints, disputes, audit, regulatory matters or legal claims	Relevant recruitment, correspondence, decision-making and supporting information	Legitimate interests. Legal obligation where applicable. Establishing, exercising or defending legal claims where relevant

6. SPECIAL CATEGORY INFORMATION

Some information needs extra protection under UK data protection law. This includes information about health, disability, race or ethnic origin, religion or belief, sexual orientation, trade union membership, genetic data, biometric data used for identification, and certain other sensitive information.

We will only use special category information where it is necessary and where a specific condition under UK data protection law applies.

We may use special category information for the following purposes:

Purpose	Special category information	Additional condition
Considering reasonable adjustments during recruitment	Disability, health or access needs	Employment, social security and social protection law
Occupational health assessments, fitness for work and pre-placement checks	Health information, medical assessment outcomes, drug and alcohol testing information and workplace adjustment information	Occupational health or assessment of working capacity. Employment, social security and social protection law
Health and safety, safety-critical work and role suitability	Health information relevant to fitness, restrictions, adjustments or safety requirements	Employment, social security and social protection law. Occupational health or assessment of working capacity
Equality monitoring and recruitment fairness reporting	Equality and diversity information	Employment, social security and social protection law and/or substantial public interest (equality of opportunity or treatment), where applicable
Legal claims, complaints or disputes	Relevant special category information where necessary	Establishing, exercising or defending legal claims

Where required, we maintain appropriate policy documentation and safeguards for special category information. This includes appropriate safeguards for special category information, such as limiting access and using the information only for the relevant recruitment, employment, safety, equality or legal purpose.

7. CRIMINAL OFFENCE INFORMATION AND VETTING

We may process criminal offence information, criminal records information or vetting information where this is necessary for a role and where WWU is legally permitted or required to do so.

This may include information obtained through the Disclosure and Barring Service, security screening providers, government vetting bodies, professional or regulatory bodies, or other authorised sources.

We will only request this information where it is relevant to the role. For example, checks may be required for roles involving critical national infrastructure, safety-critical activities, restricted sites, regulated work, sensitive systems, high levels of trust or specific legal or regulatory requirements.

Criminal offence information will only be accessed by people who need it for recruitment, vetting, legal, compliance or safeguarding purposes. We apply additional safeguards when handling this information.

Where required, we maintain appropriate policy documentation and safeguards for criminal offence information.

8. PRE-EMPLOYMENT CHECKS

If we make you an offer, the offer may be conditional on completing relevant checks. These will vary depending on the role. We will only carry out checks that are relevant and proportionate for the role.

Checks may include:

- identity checks;
- right to work checks;
- reference checks;
- qualification, licence or professional registration checks;
- employment history checks;
- occupational health or fitness for work checks, including health declarations;
- pre-placement medical assessments, where required;
- drug and alcohol testing, following a conditional offer;
- security screening or national security vetting;
- criminal record checks, where relevant and permitted by law;
- checks needed to set up employment, payroll, pensions, benefits and access to WWU systems.

We will tell you if a check is required and what information is needed. Some checks may be carried out by third party providers on our behalf. Where a third party carries out a check, we will tell you what information is needed and, where appropriate, who is carrying out the check.

9. WHO WE SHARE YOUR INFORMATION WITH

We only share applicant information where there is a business need, legal requirement or other lawful reason to do so.

Internally, your information may be shared with:

- Recruitment and HR teams;
- hiring managers and interviewers;
- Occupational Health;
- Payroll, pensions and benefits teams, if you are successful;
- IT and system access teams, if you are successful;
- Learning and Development, where onboarding or training arrangements are needed;
- Legal, Data Protection, Audit, Compliance, Cyber Security, Health and Safety or Security teams, where their involvement is necessary;
- managers or senior leaders involved in recruitment approval, governance or escalation.

Externally, your information may be shared with:

- recruitment agencies or recruitment partners;
- job boards, recruitment platforms or applicant tracking system providers, where these are used to manage applications;
- former employers and referees;
- background screening providers;
- occupational health providers and testing providers;
- Disclosure and Barring Service or other criminal record checking bodies;
- government departments or authorised vetting bodies;
- professional bodies, regulators, certification bodies or licensing organisations;
- payroll, pension, benefit, HR system or IT service providers, if you are successful;
- legal advisers, insurers, auditors, courts, tribunals, regulators or law enforcement bodies where required or appropriate;
- suppliers who provide recruitment, assessment, onboarding, HR, IT or information security services on our behalf.

We use recruitment, HR, assessment, onboarding, IT and information security systems to receive applications, manage shortlisting, arrange interviews, record decisions, complete checks and support onboarding. These systems may be provided or supported by third-party suppliers. Where suppliers process applicant information on our behalf, they must protect it and only use it for the purposes we authorise.

10. INTERNATIONAL TRANSFERS

We do not routinely transfer applicant information outside the UK.

Some service providers may store or access information outside the UK where this is necessary to provide their services. Where this happens, we will ensure appropriate safeguards are in place in line with UK data protection law. These may include UK adequacy regulations, an International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another approved transfer mechanism.

We keep this under review as part of our supplier due diligence and contracting arrangements.

11. AUTOMATED DECISION-MAKING AND AI

We do not make recruitment decisions based solely on automated processing where the decision would have a legal or similarly significant effect on you.

Recruitment decisions are made by appropriately authorised people who consider relevant information as part of the recruitment process.

We may use systems or tools to support recruitment administration, such as receiving applications, managing shortlisting workflows, scheduling interviews, recording recruitment outcomes or producing reports. We do not use AI or automated tools to make, rank, shortlist or reject applications without meaningful human involvement unless we provide you with further information. Where AI-assisted tools are used to support administrative aspects of recruitment, decisions affecting applicants will continue to involve meaningful human review.

12. HOW WE PROTECT YOUR INFORMATION

We take the security of applicant information seriously.

We use technical and organisational controls to protect personal information from accidental loss, unauthorised access, misuse, alteration or inappropriate disclosure. These include access controls, role-based permissions, secure storage, contractual controls with suppliers, staff training, audit trails and other information security measures.

Access to recruitment and occupational health information is limited to people who need it for their role. Occupational health information is handled with additional care because it may include health information and other sensitive details.

If there is a personal data breach affecting your information, we will assess the risk and take appropriate action. Where required, we will notify the Information Commissioner's Office and affected individuals.

13. HOW LONG WE KEEP YOUR INFORMATION

We keep applicant information only for as long as it is needed for the purpose for which it was collected, or where we need to keep it for legal, regulatory, audit, security or claims reasons.

In general:

- if your application is unsuccessful, recruitment records are usually retained for one year after the end of the relevant recruitment process - this period enables us to respond to recruitment queries, complaints, audit requirements and potential legal claims arising from the recruitment process;
- if you are successful, relevant recruitment and onboarding information will be transferred to your employment record and retained in line with the Employee Privacy Notice and WWU retention rules;
- occupational health records, medical assessment records, drug and alcohol testing records, health surveillance records and safety-critical records may be retained for different periods depending on the type of record and legal or health and safety requirements;
- security screening, national security vetting and right to work information may be retained for periods required by law, regulation, security requirements or WWU retention rules;
- complaint, investigation, audit or legal claim records may be retained for longer where necessary.

More specific retention periods are set out in WWU's retention rules and depend on the type of record, the role applied for and any legal, regulatory, security, health and safety or claims requirements.

WWU does not currently operate a general applicant talent pool. If this changes in future, we will provide further information.

14. IF YOU DO NOT PROVIDE INFORMATION

You are not required to provide personal information during the recruitment process unless we tell you that specific information is required.

However, if you do not provide information we reasonably need, we may not be able to assess your application, progress your application, make an offer, carry out required checks, or complete onboarding.

For example, if you do not provide information needed to check your right to work in the UK, we may be unable to employ you. If you do not provide information needed for a role-specific occupational health, safety, vetting or regulatory check, we may be unable to confirm your suitability for that role.

Where information is optional, such as some equality monitoring information, we will make this clear.

15. YOUR RIGHTS

You have rights under UK data protection law. Depending on the circumstances, you may have the right to:

- access the personal information we hold about you;
- ask us to correct inaccurate or incomplete information;
- ask us to delete information in certain circumstances;
- ask us to restrict how we use your information;
- object to processing based on legitimate interests;
- ask us to transfer certain information to you or another organisation;
- withdraw consent where we rely on consent (note that we do not generally rely on consent as a basis for processing applicant information, although consent may be requested in limited circumstances).

Where we rely on legitimate interests, we have considered and balanced any potential impact on applicants and are satisfied that our interests are not overridden by your rights and freedoms, and you can object to us using your information and we will consider your objection.

These rights do not apply in every situation. If we cannot fulfil your request, we will explain why.

We may need to confirm your identity before responding to a request.

16. KEEPING YOUR INFORMATION ACCURATE

Please tell us if information you have provided during recruitment changes or if you become aware that information we hold is inaccurate.

This helps us keep recruitment records accurate and avoid errors during the recruitment, pre-employment and onboarding process.

17. QUESTIONS, CONCERNS AND COMPLAINTS

If you have any questions about this notice or how WWU uses your personal information, please contact:

Data Protection Officer

Wales & West Utilities Limited
Wales & West House
Spooner Close
Celtic Springs
Coedkernew
Newport
NP10 8FZ

Email: dataprotection@wwutilities.co.uk

You also have the right to complain to the Information Commissioner's Office, which is the UK supervisory authority for data protection.

ICO website: [Information Commissioner's Office](https://ico.org.uk)

ICO telephone: 0303 123 1113

We encourage you to contact us first if you have any concerns, so we can try to resolve them.

18. CHANGES TO THIS NOTICE

We may update this notice from time to time. If we make significant changes, we will make the updated version available through appropriate channels.

Last updated: September 2026