Amey Recruitment Privacy Notice

Your privacy, our promise

At Amey, we handle personal information fairly, transparently and responsibly. This notice explains how we collect, use and protect personal data about people who apply for roles with Amey or are considered for opportunities with us. It is designed to help you understand how we use your personal information. If you are applying for a role at one of our group companies outside of the UK, please read this notice together with any country specific recruitment information that applies to you (see the additional sections at the end).

Who we are

We are Amey. We act as the data controller for the personal information we collect and use about you during the recruitment stage. If you apply through an agency, they act as a separate controller for the information you give them directly and we encourage you to also read their privacy notice.

If you are applying for a role outside of the UK at one of our international Group companies, please read the relevant country-specific additional information below. This explains which Group company is involved in the recruitment process for that location.

Who this notice applies to

This notice applies to anyone who:

- applies for a role with Amey;
- is identified or approached by Amey or by a third-party acting on our behalf as a potential candidate;
- is put forward by a recruitment agency;
- takes part in interviews, assessments or selection activities;
- is included in a talent pool or future opportunity database; or
- responds to our social media recruitment campaigns.

It applies whether you apply directly, via an agency, through our careers site, or through other recruitment platforms.

Our site is not intended for children, and we do not knowingly collect data relating to anyone under the age of 16.

What we collect – only what is needed

- **Identification and contact information**
  Name, contact details, address, date of birth, right-to-work/eligibility information.
- **Recruitment and career information**
  CVs, application forms, employment history, education, qualifications, skills, experience, interview notes.
- **Assessment information**
  Results of interviews, tests or selection activities undertaken during the recruitment process.

Why we collect your data (what we use it for)

We only ask for what we need. We use your information to:

- assess your suitability for the specific role you applied for or similar roles with Amey;

- manage recruitment and selection for the role you've applied for (applications, interviews, assessments, scheduling);
- provide you with reasonable adjustments to the recruitment process, where necessary
- communicate with you about your application;
- carry out background checks at the conditional offer stage (see "Background checks and screening" below);
- meet legal and regulatory obligations (e.g., right-to-work, safeguarding, health & safety);
- keep appropriate records of recruitment decisions related to your application and the specific role considered;
- improve, monitor and secure our recruitment processes, including those you participate in;
- run psychometric testing when assessing candidates in larger scale recruitment drives, including if your role is part of such a process (e.g., early careers);
- use AI to support our processes, for example using assisted notetaking during interviews to capture what was discussed (all final decisions are made by human reviewers); and
- in aggregate form (not at an identifiable to you) to help us understand where best to promote our vacancies, including on social media.

Our legal reasons for using your data

We use your personal information where it is necessary to:

- take steps before entering into a contract with you and, where relevant performance of a contract (for example, to assess your application and arrange interviews);
- comply with legal obligations, for example:
    - immigration/right-to-work checks
    - safeguarding/criminal record checks if a role requires them (e.g., if the role you're applying for requires you to work with vulnerable groups or within regulated/sensitive environments)
    - health and safety obligations (e.g., drugs & alcohol testing for safety critical roles)
    - other regulatory or client mandated checks needed for specific projects, sites or contracts (e.g. background checks required by a client before working on a secure government project site); and
- pursue our legitimate interests in running fair, safe and effective recruitment (e.g., using an approved agency list, psychometric tools, AI-assisted notes, and shortlisting support).

We rely on consent only where participation is genuinely optional (e.g., responding to diversity monitoring questions).

If you would like more detail regarding the reasons why we use your personal data, please email privacy@amey.co.uk.

How we collect your information

- Directly from you (applications, CVs, interviews, assessments).
- Approved recruitment agencies and search firms where you have applied for a role through them or asked them to share your details with us.
- Referees you have provided in connection with your application (where applicable).
- Public/professional sources relevant to the role you have applied for (e.g., LinkedIn).
- Recruitment platforms/systems we use to manage your application.
- Job alerts/talent pools you sign up for.
- Social media recruitment campaigns (if you respond or submit details).

Using our careers website and recruitment systems

When you use our careers site or recruitment systems, we also collect limited technical data (e.g. IP address, browser type, usage data) to keep services secure and improve the experience. Please view our Cookie Notice for details.

Our main online platform provider is SAP (UK) Limited (SAP SuccessFactors). We also work with selected testing and assessment providers, such as Neurosight, Korn Ferry Assessment and Thomas International, and with a credit reference agency for finance/credit screening where relevant. These providers act under our instructions and meet our security and confidentiality requirements.

Background checks and when they happen

We carry out screening after a conditional offer is made (unless local law requires earlier checks). Checks may include:

1. Employment references;
2. Right-to-work & ID verification;
3. Criminal record checks where legally required (e.g., DBS/ Disclosure in Scotland in the UK, Garda Vetting or equivalent in Ireland) with your authorisation;
4. Drugs & alcohol testing for safety critical or high-risk roles (and will continue during employment in line with policy and law);
5. Finance/credit or anti-fraud checks where relevant to the role (e.g., roles with significant financial responsibility); and
6. Pre-employment health checks and occupational health assessments where relevant
7. Eligibility to drive (if applicable to the role you're applying for)
8. other screening required by law, or where necessary or proportionate due to client requirements or the nature of the position.

We decide which roles require screening based on:

- legal obligations (e.g., safeguarding laws, right-to-work, security/regulatory site access, health & safety rules for safety critical work);
- client or contractual obligations; and
- Role specific risks (e.g., access to funds or sensitive information).

If you do not authorise the required check, the required check cannot be completed, or you do not meet the necessary standard, your conditional offer may be withdrawn.

Equality, diversity and inclusion (optional)

We may invite you to share diversity information (e.g., gender, ethnicity, disability, sexual orientation) at the application stage and again later to confirm accuracy. Providing this information is completely optional and will not affect your application. We use it to:

- monitor and improve inclusion;
- produce diversity statistics (usually anonymised/aggregated) and meet any legal reporting duties.

This information is kept separate from your application and is only accessed by staff responsible for monitoring equality and inclusion.

How we protect your information

We use strong security measures - physical, digital, and procedural - to keep your data safe from loss, misuse, or unauthorised access. Staff who handle personal information receive training and only those who need your data to do their job can see it.

How we use AI-assisted tools

We may use artificial intelligence ('AI') technology to support the recruitment process. Typically, this can include:

- AI-assisted notetaking during interviews to help capture key points.
- Summarising interview notes and highlighting how your answers relate to key assessment areas.
- AI -assisted tools that analyse elements of your performance during an assessment and provide suggestions to our recruitment team about which candidates may be suitable to progress.

AI tools do not make final decisions about your application. All recruitment decisions are made by people, who review insights from AI technologies alongside other information. We do not make decisions solely by automated means.

Who we share your information with

We only share your information where we are legally permitted to do so. We ensure that the data that we share is proportionate and necessary. This includes:

- our approved recruitment agencies (if the specific role you applied for was managed by a recruitment agency);
- other companies in the Amey group (for example, the UK Recruitment Team where they help support recruitment for our international businesses);
- service providers who support recruitment systems and any assessments that form part of your application, where these are delivered by a trusted third-party;
- background screening providers (at conditional offer stage) and where relevant to the role you have applied for;
- clients where a role or site requires client approval or additional checks;

- professional advisers if necessary; and
- regulators or authorities where required by law.

When we work with third-party providers; for example, recruitment systems, assessment providers or background screening companies that carry out activities on our behalf, we carry out appropriate security and due diligence checks to make sure your information is protected and used only in line with our instructions.

Regardless of the need for sharing your information, we share only the minimum information needed for the purpose.

International transfers

Amey operates internationally, and we may share your information with other Amey group companies or with trusted suppliers based outside the UK.

In some cases, this will involve an international transfer of your personal data, for example where we use global recruitment systems or specialist providers based outside the UK.

Where this happens, we make sure the appropriate safeguards are in place to protect your information and to ensure it continues to be handled in line with applicable data protection laws.

For more specific information about how international transfers apply to your location, please see the country specific recruitment privacy information below.

How long we keep your information

We keep recruitment data for only as long as needed for recruitment and legal purposes. Typically:

- Unsuccessful candidates: we typically retain your personal information for 18 months from the date you were notified of the outcome or from 18 months after you last logged in or engaged with your candidate account. After this period, your personal information is deleted or anonymised in line with applicable laws.
- Successful candidates: relevant information is transferred into your staff record (you will be invited to view our Staff Privacy Notice after you have accepted our offer of employment).
- Talent pools: if you opt in, we retain your details longer to let you know about future opportunities. You can opt-out at any time, at which point your information will be retained for up to 18 months after you have opted out.

Your rights – you are in control

Depending on where you are based, you may have the right to:

- ask what information we hold about you;
- correct anything that's wrong;
- ask us to delete data we no longer need;
- withdraw consent (where we rely on it);
- not be subject to automated decisions or profiling without human review;
- object to how we use your data;
- ask us to restrict or transfer your data; and

- complain to us and, if necessary, your local data protection authority.

You may contact us at any time to exercise your rights by emailing Privacy@amey.co.uk. Doing so will not affect your application.

We aim to respond within one month, or as required by local regulations, and will keep you informed of our progress.

Change of purpose

We will only use your personal information for the reason we collected it. If we ever need to use it for a different reason, we will always consider whether another purpose is compatible before using your information in a different way. We will never use your personal information for an incompatible purpose e.g. adding your email address to our client marketing database.

If we need to use your information for a purpose that is not compatible, we will tell you and explain the legal reason for doing so. In some situations, the law may allow or require us to use your information without notifying you.

Informing us of changes to your data

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your recruitment process by contacting us using the details in the Contact us section below.

Change of purpose

If you have questions or want to exercise your rights, contact our Privacy Team:
Email: privacy@amey.co.uk
Post: Privacy Team, Amey, The Matchworks, Speke Road, Liverpool L19 2PH

Updates to this notice

We review this notice regularly to keep it accurate and relevant. It was last updated on March 2026.

Glossary

See here.

Annex A - Country Specific Recruitment Privacy Information

The following additions form part of the Amey Global Recruitment Privacy Notice and apply in addition to the main notice above. If there is a conflict between the main notice and the information below, the country specific information applies to candidates applying for a role within that country.

1. United Kingdom – Recruitment Privacy Information

If you're applying for a role with Amey in the UK, this section provides extra information that applies alongside the main notice.

Background checks and medical assessments

We generally carry out background checks at the conditional offer stage, but in some cases we may need to complete them earlier where required by law, client or site rules, or to meet security vetting timelines.

For UK based roles, where applicable, we carry out criminal record checks through:

- the Disclosure and Barring Service (DBS)
- Disclosure Scotland (including PVG Scheme checks where required)
- Access NI (where relevant)

We only ask for the level of disclosure needed for the role, and we follow the *Rehabilitation of Offenders Act 1974* when considering the relevance of any information disclosed.

For certain UK roles, typically those involving safety critical work, driving, rail, defence or other high-risk environments, we carry out drugs and alcohol testing at the conditional offer stage. Ongoing testing may also apply after you join, where required by law or policy, to ensure we operate safely.

Due to the nature of work carried out for our clients, some UK roles may also require additional checks such as:

- enhanced government security vetting (e.g., Baseline Personnel Security Standard, Counter Terrorist Check, Security Check, Developed Vetting)
- financial or anti-fraud checks for roles with financial responsibility

These checks are only carried out where relevant to the role, and you will be informed before applying if these checks are a required condition of employment.

Right to work checks

UK law requires us to confirm that you have the legal right to work in the UK before employment begins. This involves verifying your passport, immigration status or other approved documents in line with Home Office guidelines. We are legally required to keep a record of these checks.

Supervisory authority

The supervisory authority for data protection in the UK is the Information Commissioner's Office (ICO).
Website: www.ico.org.uk

2. The United States – Recruitment Privacy Information

Amey Consulting USA Inc (incorporated in Delaware) operates in the USA and manages Amey activity in the United States (US). If you're applying for a role with Amey in the US, this section provides extra information relevant to your recruitment experience. It should be read together with the main Group Recruitment Privacy Notice.

Recruitment activities for roles with Amey Consulting USA Inc are supported and managed by Amey UK. When using your personal data to process your application, we adhere to relevant federal and state data protection and security laws.

Background checks

To verify your right to work in the United States, we will ask you to provide the information needed to complete Form I-9 (Employment Eligibility Verification), after an offer of employment is made. You will receive a clear disclosure and be asked to provide written authorisation before any consumer report is requested. If a background check is required, it will be carried out only after you have accepted a conditional offer, unless applicable law allows or requires them at an earlier stage of the recruitment process. Background checks will be conducted by a third-party provider in accordance with the Fair Credit Reporting Act (FCRA). If information from a background check may negatively affect your application or employment, you will receive the required pre-adverse action notice, a copy of the report, and a summary of your rights, including your ability to dispute its accuracy.

Who we share your data with

In addition to the information provided in the main recruitment privacy notice, if you are applying for a role in the US, we may also be required to share your personal data with US state, federal and local governmental agencies, regulators, screening providers, or other third parties where this is necessary to comply with legal requirements, verify work eligibility, carry out lawful background screening, or support the recruitment and onboarding process.

International Transfers

Your data may be processed in:

- The United States, including the state where the role, hiring team, or service providers are based.
- The United Kingdom, where Amey UK supports recruitment and onboarding.
- Other countries, where relevant Amey Group teams or service providers operate.

When data is shared between locations, we ensure it is handled safely and in line with applicable data-protection laws, using agreed data-sharing practices and safeguards across the Amey Group.

Equal employment opportunity (EEO) data (optional)

In addition to the diversity monitoring questions asked to all candidates, in the US, we may also ask for information such as veteran status, or other diversity-related information where this is relevant to equal employment opportunity monitoring, reporting or compliance. Providing this information will not affect your application.

We process this information in accordance with applicable United States employment and anti-discrimination laws. Where US state privacy laws require consent for certain uses of sensitive personal information, we will request it.

Your rights

The rights described in the main Recruitment Privacy Notice reflect Amey's global approach to managing personal data. Because the U.S. does not have one nationwide data protection law, and state rules can differ, the rights available to applicants may vary depending on the situation and the laws that apply.

How we respond to your rights will depend on the privacy requirements of the relevant state, which may be the state where you live or the state in which we are operating. When specific legal rights apply, we will follow those requirements. We aim to handle all requests fairly and transparently, and we will explain the outcome if we are unable to fulfil a request.

We do not sell candidate personal information or share candidate personal information for cross-context behavioural advertising. When we run online recruitment campaigns (for example, with Meta), we may use aggregate, non-identifiable information to help us understand the effectiveness of our advertising. This does not allow Meta or any other company to target you as an individual.

Contact Us

If you have any questions about this Privacy Notice, how we handle your personal information, or if you wish to exercise your data protection rights, you can contact us at:

Privacy@amey.co.uk

All enquiries are handled by the Amey Privacy team based in the UK.

You may also raise concerns with the relevant US regulator. Depending on your location your privacy-related concerns may be raised with relevant United States authorities, such as the Federal Trade Commission (FTC) or your State Attorney General, depending on where you live.

3. Ireland – Recruitment Privacy Information

Amey Ireland operates in the Republic of Ireland and manages Amey activity in Ireland. If you're applying for a role with Amey in the Republic of Ireland, this section provides extra information that applies alongside the main global recruitment privacy notice.

International transfers – Ireland

Recruitment for our Irish entities is centrally supported by the Amey UK Recruitment Team, which means your information may be accessed in the UK. The UK currently has an EU adequacy decision, which means your data is protected to EU standards.

If we transfer your information to countries outside the European Economic Area (EEA), we apply the safeguards required under the EU GDPR, such as Standard Contractual Clauses or other approved mechanisms.

How we use AI tools

We take steps to ensure that our use of AI tools, whether inside or outside of Ireland, complies with the EU AI Act. This includes not using AI for prohibited practices such as emotion recognition in the workplace or biometric categorisation that infers protected traits. We are committed to ensuring we meet our obligations under the EU AI Act at each stage that they take effect.

Background checks and medical assessments

We generally carry out these checks at the conditional offer stage, unless required earlier by law, client/site rules, or to meet vetting timelines.

For roles based in Ireland, background checks may include:

- Garda Vetting through the National Vetting Bureau (where required by law or the role)
- Employment references
- Right to work and identity verification
- Qualifications and professional membership checks

We only request Garda Vetting where it is legally required, for example for roles involving work with vulnerable people or in regulated environments. Garda Vetting is carried out in line with the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012–2016.

For certain roles, typically those involving safety critical duties, driving or work in high-risk environments, we may also carry out drugs and alcohol testing at the conditional offer stage. Testing may also continue after you join, where required by law or client site rules.

Due to the nature of the work Amey provides to clients in Ireland, additional checks may also apply, such as:

- security or site access checks
- financial or anti-fraud checks for roles with financial responsibility.

These checks are only carried out where relevant to the role, and you will be informed before you apply if they are a condition of a job offer.

Right to work checks

Irish law requires us to confirm that you have the legal right to work in Ireland before employment begins. This involves checking your passport or national identity document, verifying any immigration permissions where relevant, and confirming any required employment permits. We are legally required to keep a record of these checks.

Supervisory authority

If you are based in Ireland, your supervisory authority for data protection is the Data Protection Commission (DPC).
Website: www.dataprotection.ie