SMART MANUFACTURING TECHNOLOGY
PRIVACY NOTICE
(INTERNAL)

Published: 11th November 2026

CONTACT DETAILS

Contact: Privacy Team

Address: 1 Clifton Lane, Wilford, Nottingham, NG11 7AT

E-mail: privacy@smartmt.com

Website: smartmt.com

INTRODUCTION

We are Smart Manufacturing Technology (SMT), a global engineering solutions and services provider dedicated to providing leading engineers with the expertise and tools to deliver innovative powertrain technology. Our Head Office is in Nottingham, UK. SMT maintains registration with the Information Commissioner's Office (ICO).

This notice explains how we collect and use personal data during the employment and engagement lifecycle, including recruitment and assessment, onboarding, employment or contracting, benefits and payroll, learning and development, IT and security operations, and premises security including CCTV. It applies to employees, contractors and candidates. For customers, prospects, website visitors, suppliers and other external contacts, see our External Privacy Notice.

Your privacy and the security of your information are responsibilities that SMT takes seriously. We understand our responsibility to ensure that any personal data we collect, store, use or otherwise handle is processed in accordance with applicable data protection legislation.

THE TYPES OF PERSONAL DATA WE COLLECT

At SMT, we only collect the personal data necessary to manage recruitment and the employment or engagement lifecycle, meet our legal and contractual obligations, operate and protect our business, systems and premises, and undertake necessary internal business functions.

We need to keep appropriate records throughout recruitment and the employment or engagement lifecycle to manage our relationship with candidates, employees and contractors.

Where personal data is required to enter into or perform an employment or engagement contract, administer payroll or benefits, provide access to SMT systems or premises, or meet a legal obligation, failure to provide it may mean that SMT cannot progress an application, enter into or administer the relevant employment or engagement, provide access, or meet the applicable requirement. Information identified as optional does not have to be provided.

The personal data that we collect includes

- **Identifiers and contact information**: names, addresses, email addresses, telephone numbers, date of birth, signatures, emergency-contact details, photographs, employee or contractor identifiers, usernames and hostnames.
- **Employment and background information**: CV, education and work history, references, right-to-work and identity documents, qualifications and professional memberships.
- **Employment and engagement records**: contract, role, working arrangements, attendance, leave, performance and progression, learning and development, disciplinary and grievance information.
- **Payroll and benefits**: bank details, tax and payroll information, pension information and benefit selections.
- **IT, security and premises**: account, device, network and access information associated with the use of corporate systems and devices, photographs, access-control records and CCTV footage.
- **Travel and driving**: driving licence and eligibility, visas and information necessary for business travel.
- **Special-category data, where relevant and permitted**: health information, including sickness, workplace-adjustment and occupational-health information, and equality-monitoring information collected for legal, reporting or inclusivity purposes.

This list is non-exhaustive and, where necessary and appropriate to our relationship with you, we may collect additional personal data from you, former or current employers, referees, recruitment agencies, education or professional bodies, public authorities, service providers, or other relevant third parties.

HOW WE GET THE PERSONAL DATA AND WHY WE HAVE IT

Most of the personal data we process is provided directly by you during recruitment, onboarding and throughout your employment or engagement. We may also receive personal data indirectly from:

Recruitment agencies and referring partners in connection with employment opportunities.

Former or current employers and referees to obtain references or verify employment information.

Universities, education providers and professional bodies to verify qualifications or administer learning and development.

Government departments and public authorities where necessary for tax, immigration, legal or regulatory purposes.

Restricted - External

SMT systems and service providers where information is generated through the use of corporate systems, devices or premises.

We use this data for the following purposes:

- **Recruitment and onboarding:** assessing suitability, verifying identity and right to work, and processing offers and contracts.
- **Employment and contractor administration:** payroll, pensions, benefits, attendance, working arrangements, performance and progression, learning and development, health and safety, and internal record-keeping.
- **IT, security and premises operations:** identity and access management, device and network administration, safeguarding systems and data, managing site access and maintaining premises security.
- **Legal and regulatory obligations:** meeting tax, employment, immigration, health and safety and other legal requirements, and responding to lawful requests.
- **Protecting SMT's rights and interests:** investigating suspected misconduct, security incidents or legal claims and protecting SMT personnel, information, systems and assets.

THE LAWFUL BASES WE RELY ON FOR PROCESSING PERSONAL DATA ARE:

We rely on one or more of the following lawful bases, as appropriate to each activity:

(a) Your consent. Only where requested for optional processing. You may withdraw consent at any time using the mechanisms described in this notice.

(b) We have a contractual obligation. To take steps before entering into, or to perform, your employment contract or other contract of engagement.

(c) We have a legal obligation. For example, employment, tax, immigration, equality, health and safety, and regulatory requirements.

(d) We have a legitimate interest.

For example, recruitment and workforce management; business administration and internal record-keeping; learning and development; IT and information security; proportionate monitoring of systems and premises; investigating suspected misconduct, security incidents or legal claims; and protecting SMT's personnel, information, systems, premises and assets.

(e) We have a vital interest. It is unlikely that SMT will rely on the lawful basis relating to vital interests to process your personal data. SMT only relies on vital interests as a lawful basis where the processing or sharing of information is necessary to protect someone's life, or to avoid significant harm to life, in an emergency.

Public tasks: SMT does not rely on the lawful basis relating to public tasks, as we do not process personal data in the exercise of official authority or to perform public-interest tasks set out in law.

Special category data: Where we process special-category personal data, we rely on an appropriate lawful basis under UK GDPR Article 6 and an additional condition under Article 9 and the Data Protection Act 2018. Depending on the purpose, this may include employment, social security and social protection law, occupational health or assessment of working capacity, equality-of-opportunity monitoring, protection of vital interests, or the establishment, exercise or defence of legal claims. We restrict access to such information and apply appropriate safeguards.

Restricted - External

WHERE NECESSARY AND APPROPRIATE, WE MAY SHARE THIS INFORMATION WITH:

We share data only where necessary and with appropriate safeguards. Typical recipients include:

- **HR and people services**: banks, accountants, outsourced payroll providers, pension and employee-benefits providers, HR information-system providers, occupational-health and health and safety providers, recruitment providers, and relevant professional consultancies.
- **IT and information security providers**: e.g., Microsoft and outsourced IT and Security solutions partners, including CCTV monitoring providers.
- **Professional/insurance services**: consultants and advisors, auditors, certification bodies, and insurers.
- **Legal and regulatory authorities**: law enforcement, tax authorities, courts and regulators when required by law.
- **Corporate transactions**: prospective buyers and their agents in the context of a business sale or reorganisation.

SMT and some of its service providers operate internationally. This may involve transferring personal data outside the UK or European Economic Area, including to countries that are not covered by a UK or EU adequacy decision.

Where required, SMT uses an appropriate transfer mechanism, such as the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another safeguard permitted by applicable data protection law. Where a transfer is not based on an adequacy decision, SMT assesses the transfer risks and applies supplementary measures where necessary.

HOW WE STORE YOUR PERSONAL DATA

We apply appropriate technical and organisational security measures, including encryption where appropriate and secure disposal of data storage media in accordance with recognised industry standards. Physical records are securely destroyed.

Unless data must be deleted sooner, or a longer period is necessary for a specific legal, contractual, accounting, insurance, employment, health and safety or dispute-management purpose, physical and electronic records shall be retained for the following periods, at the end of which they are securely disposed of or put beyond use.

- **Recruitment and employment records:** retained in accordance with SMT's Records Retention Schedule, taking account of applicable statutory requirements and relevant CIPD guidance.
- **Financial documents, payroll-supporting timesheets and attendance records:** normally six years plus the current financial year.
- **Insurance and associated health and safety records**: retained for the period specified in SMT's Records Retention Schedule according to the nature of the record, insurance requirement and potential claims.
- **CCTV footage:** normally 30 days, or up to 365 days following completion of an investigation where the footage is required as evidence.
- All physical records containing personal data are disposed of by secure information disposal methods in line with applicable standards and regulations.

Restricted - External

- All data storage media, including hard drives, USB drives and disks, are securely wiped or factory-reset, as appropriate, before the internal reuse of an associated device. Before external recycling or sale, data storage media are securely wiped in accordance with recognised industry standards or permanently destroyed.
- Archived physical records clearly display the scheduled destruction date.

DATA SUBJECT RIGHTS

Under data protection law, data subjects have rights including:

Your right of access – You have the right to ask us for copies of your personal data.
Your right to rectification – You have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
Your right to erasure – You have the right to ask us to erase your personal data in certain circumstances.
Your right to restriction of processing – You have the right to ask us to restrict the processing of your personal data in certain circumstances.
Your right to object to processing – You have the right to object to the processing of your personal data in certain circumstances.
Your right to data portability – You have the right to ask that we transfer the personal data you gave us to another organisation, or to you, in certain circumstances.
Your rights in relation to automated decision-making and profiling – You have rights in relation to decisions based solely on automated processing, including profiling, where those decisions produce legal or similarly significant effects. SMT does not currently make decisions about individuals based solely on automated processing where those decisions produce legal or similarly significant effects. If this changes, we will provide appropriate information about the processing, its significance and the likely consequences.

The rights available to you depend on the circumstances and the lawful basis on which we process your personal data. Where processing is based on your consent, you have the right to withdraw that consent at any time.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. Please contact us at privacy@smartmt.com if you wish to exercise your data subject rights.

CHANGES TO THIS NOTICE

We may update this notice from time to time and will make the most recent version available on our website.

HOW TO COMPLAIN

If you have any concerns about our use of your personal data, you can make a complaint to us at:

Privacy Team, Smart Manufacturing Technology Ltd

1 Clifton Lane, Wilford

Nottingham, NG11 7AT

Email: privacy@smartmt.com

SMT takes your privacy seriously and invite you to raise any concerns to us directly in the first instance, to allow us the opportunity to advise, and where necessary, perform any relevant investigations.

You have the right to complain directly to the ICO if you have concerns with how we are processing your personal data.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

Restricted - External