

It is important that you read this policy in full to understand the rules and practices

GDPR

General Data Protection Regulation

Employee Privacy Policy
All Metal Services Limited

16 April 2021

All Metal Services Limited Employee Privacy Policy

All Metal Services Limited (AMS) is committed to protecting the privacy and security of your personal information.

This privacy policy sets out the basis on which any personal information we collect from you, or that you provide to us, will be processed by us. It is important that you read this policy in full to understand what information we hold about you, how we may use it and what rights you have in relation to your data.

This privacy policy applies to all employees, workers, contractors and job applicants. It does not form part of any contract of employment or other contract to provide services. We may need to update this policy from time to time to reflect any changes in the law or to our business. We will always notify you of any changes we make to this policy.

Who are we

We are All Metal Services Limited, a limited company incorporated in England and Wales with company number 01559685.

Our registered address is 5 Midpoint Park, Kingsbury Road, Minworth, Sutton Coldfield B76 1AF. In this policy we refer to ourselves as “we”, “us”, “our” and “AMS”.

AMS is a “data controller”. This means that we are responsible for deciding how we hold and use personal information we have collected from you. We are entered in the Register of Data Controllers with registration number: ZB045991.

Data Protection Lead

We have appointed a Data Protection Lead (DPL) to oversee compliance with this privacy policy. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPL as follows:

The Data Protection Officer

data.protection@allmetal.co.uk

What personal information we may hold about you

Personal information means any information that can be used to identify you, either on its own, or in combination with other information directly linked to you. It does not include personal information that has been anonymised. There are also “special categories” of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as your name, previous names, title, addresses, telephone number(s), and personal email address(es)
- Date of birth
- Gender
- Identification documents such as passport, birth certificate
- Driving licence, car insurance and MOT documents (where applicable)
- Marital status and dependants
- Emergency contact and beneficiary information
- National Insurance number
- Bank account details, payroll records and tax status information

- Salary, annual leave, family and other leave, pension and benefits information
- Terms and conditions of your employment, contract of employment and any amendments to contract of employment
- Start date
- Location of employment or workplace
- Recruitment information (including copies of right to work documentation, interview notes, 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, professional qualifications, working hours, training records and professional memberships)
- Compensation history
- Performance information, including Appraisals and Performance improvement plans
- Succession information and Individual development plans
- Disciplinary and grievance information.
- CCTV footage and information obtained through electronic means such as door entry fobs, van tracking information
- Information about your use of our information and communications systems
- Photographs, video footage, and call recordings (sales and customer care only)

We may also collect, store and use sensitive personal information (also known as special categories of data), which may include:

- Information about your race or ethnicity and nationality, information about your health, including any medical condition or disability, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We typically collect your personal information through the application and recruitment process, either directly from you or sometimes from a recruitment agency or through an employee referral scheme. We will also collect additional personal information about you during job-related activities throughout the period of your employment with us. You will usually provide information directly to your managers or colleagues, our HR or Payroll department, or enter it into our systems for example through Employee Self Service.

We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies, government agencies, local authorities and HMRC.

If you provide any personal information relating to another person, for example a spouse or next of kin, we assume that you do so with their full knowledge and consent.

Data is stored in a range of different places, including your personnel file, our HR and Payroll systems (Tensor and Access) and other IT systems, e.g. the company's email system.

If you do not provide personal information

We may need to collect personal information by law, or under the terms of the employment contract we have with you. If you do not give us this information when requested, we may be prevented from performing the contract we have entered into with you (such as paying you your salary 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).

Our purpose for collecting and processing your personal information

Data Protection law says that we can use your personal information only if we have a lawful purpose for doing so. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you
- Where we need to comply with a legal obligation

- 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

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

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

We need all the categories of information in the list above (see "What personal information we hold about you" above) primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. Sometimes we may use your personal information to pursue our legitimate interests or those of third parties, provided your interests and fundamental rights do not override those interests. A legitimate interest is when we have a business or commercial reason to use your information.

Here is a list of all the ways in which we may process your personal information and which of the lawful purpose(s) we are relying on to do so. Some of the grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Purpose	Lawful basis
Making a decision about your recruitment or appointment:	Our legitimate business interests to ensure you are suitable for the role. For defence against potential legal claims.
Assessing qualifications for a particular job or task, including decisions about promotions:	Our legitimate business interests to ensure you are suitably qualified to perform your job and to assess any training needs. To ensure our business operates effectively.
Checking you are legally entitled to work in the UK:	To comply with legal obligations. To defend against legal claims.
Ascertaining your fitness to work:	To comply with legal obligations. Our legitimate business interests to ensure your health and safety in the workplace and to provide appropriate workplace adjustments.
Administering the contract we have entered into with you:	To allow us to perform our contract with you and to comply with legal obligations.
Paying you and, if you are an employee, deducting tax and National Insurance contributions:	To allow us to perform our contract with you and to comply with legal obligations.
Including but not limited to providing, the following benefits to you: (where applicable) <ul style="list-style-type: none"> • Medical insurance • Life assurance • Car allowance • Pension • Holiday including Buy and Sell holiday • Voluntary dental insurance • Cycle to work scheme • Share option plans • Give as you earn plan • Childcare vouchers • Referral schemes • Educational sponsorship including Merit awards 	To allow us to perform our contract with you and to comply with legal obligations.

Liaising with your pension provider:	To allow us to perform our contract with you and to comply with legal obligations.
Making decisions about salary reviews and compensation:	To allow us to perform our contract with you and our legitimate business interests around effective business management and performance.
Carrying out salary benchmarking reviews:	<p>Our legitimate business interests. Benchmarking allows us to determine that our salaries are in line with industry standards so that we can retain and attract the best candidates.</p> <p>To comply with legal obligations: we may need to review and report on salaries between different candidates performing the same role e.g. for Gender Pay Gap purposes.</p>
Conducting performance reviews, managing performance and determining performance requirements:	To allow us to perform our contract with you. Our legitimate business interests around performance, capability and training and to enable us to operate effectively. To defend the business against legal claims.
Education, training and development requirements:	To allow us to perform our contract with you and our legitimate business interests to ensure suitability for the role and to identify any training needs.
Making decisions about your continued employment or engagement:	To allow us to perform our contract with you and our legitimate business interests about effective business management.
Administering your expense claims:	To allow us to perform our contract with you and to comply with legal obligations.
Managing sickness absence:	To comply with legal obligations. To calculate sick pay. Our legitimate business interests around ensuring 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.
Managing maternity or paternity or adoption leave:	To comply with legal obligations.
Gathering evidence for possible grievance or disciplinary hearings.	To comply with legal obligations. Our legitimate business interests around investigating conduct or capability issues and to defend against legal claim.
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	To comply with legal obligations. Our legitimate business interests around investigating conduct or capability issues and to defend the business in any legal claims.
Equal opportunities monitoring:	To comply with legal obligations. Our legitimate business interests to ensure meaningful equal opportunity monitoring and reporting.
Capture CCTV footage for security purposes.	Our legitimate interests around health and safety and crime prevention.
Complying with health and safety obligations:	To comply with legal obligations. Our legitimate business interests to ensure your health and safety in the workplace.

To prevent fraud:	To comply with legal obligations.
To monitor your use of our information and communication systems to ensure compliance with our IT policies:	To comply with legal obligations. Our legitimate business interests around crime prevention and to protect against misuse or damage to our IT systems. To assist in the investigation of alleged wrongdoing.
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution:	Our legitimate interests around crime prevention. To ensure effective communication and working practices within the business. To protect against misuse of IT and communications systems. To defend against legal claims.
Business management and planning, including accounting and auditing:	To comply with legal obligations. Our legitimate interests to understand how we are performing so we can meet our mission statement and objectives and to help us to monitor our performance.
To conduct data analytics studies to review and better understand employee retention and attrition rates:	Our legitimate interests to evaluate our business and its culture.

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 sensitive personal information

“Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for processing this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations.
- Where it is needed in the public interest, such as for diversity and inclusion monitoring and reporting or in relation to our occupational pension scheme.
- Where it is needed to assess your working capacity on health grounds, such as drug and alcohol testing, subject to appropriate confidentiality safeguards.

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.

We will only use your sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other legislation.
- 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.
- We will use information about your race or ethnicity, nationality, religious beliefs and/or sexual orientation to ensure meaningful equal opportunity monitoring and reporting.

We do not need your consent to process your sensitive personal information where we process it to carry out our legal obligations or to exercise specific employment law rights. 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 why 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.

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.

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 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.

We are no longer collecting information about criminal convictions. Any information of this type that we do hold about you is in the process of being destroyed. When records are destroyed, whether held as paper records or in electronic format, we will ensure that they are safely and permanently erased.

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:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- 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 based on any 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.

Who has access to data

Your information will be shared internally, including with members of the HR and Payroll team, Directors, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles. We may also share your data with Directors, Line Managers and respective PA's where there is a legitimate personal reason to do so (such as sending cards and gifts).

Data sharing

We may 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. When sharing information, we will comply with all aspects of data protection law.

Where the information is of a sensitive nature, for example about your health, we will generally obtain consent from you prior to sharing this information, unless we are required or permitted to share this by law.

Which third-party service providers process my personal information?

We may share your personal information with the following third parties providing services on our behalf:

- Our service providers for the following purposes:
 - For the provision and administration of your pension and life insurance
 - For the provision and administration of your benefits
 - For the provision and administration of payroll and HR services
 - For the provision and administration of a company car or our vehicle fleet
 - For the provision of carrying out salary benchmarking reviews
 - To obtain or provide employment references
 - Recruitment service providers
 - Occupational health providers
 - Specialist consultants and legal advisors
 - Learning and training providers
 - Internal and external auditors
 - Document storage solutions
 - Electronic signature solutions
- HM Revenue and Customs in relation to the collection of tax or duty.
- Police and other relevant authorities (e.g. Department of Work & Pensions, Probation Service,) in relation to the prevention and detection of crime, the apprehension of offenders or the collection of tax or duty.
- Our legal advisors in relation to the defence of legal claims
- Reliance Steel and Aluminum (RSAC)

We may also share information when required by law for example where ordered by the Court or to protect an individual from immediate harm.

How secure is my information with third-party service providers and other entities in our Group?

All our third-party service providers and other entities in the Group 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.

When might you share my personal information with other entities in the group?

We may also share your personal information if the structure of AMS changes in the future. We may choose to sell, transfer, or merge parts of our company, or our assets; or we may seek to acquire other companies or merge with them. During any such restructuring of our Group, we may share your information with other parties. We'll only do this if those parties agree to keep your data safe and private.

We will share your personal information with other entities in our Group as part of our regular reporting activities on company performance.

Sending data outside of the EEA

We will only send your data outside of the European Economic Area ('EEA') to:

- Follow your instructions or fulfil a request on your behalf (such a booking travel or overseas accommodation);
- To service providers such as providers of data hosting, IT, training, travel or employment benefits so that they can provide those services to us, acting under our instructions as data processors; or
- Comply with a legal duty.

If we do transfer your personal information outside of the EEA, we will take such steps as we are legally required to follow, to make sure it is protected in the same way as if it was being used in the UK/EEA. To do this, we will usually use one of these safeguards:

- Transfer it to a non-EEA country with privacy laws (or another legally recognised arrangement) that meets required UK and/or EEA data protection standards; and/or
- Put in place a contract with the recipient that means they must protect it to the same standards as the UK and/or EEA.

Data security

We have put in place measures to protect the security of your information. 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 employees, agents 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 keep my information?

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, 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 Document Retention Policy. 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 company we will retain and securely destroy your personal information in accordance with our data retention policy.

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 our Data Protection Lead at the contact details noted above or at data.protection@allmetal.co.uk

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 our DPL on data.protection@allmetal.co.uk. 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.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, using the following contact details:

Information commissioner

Wycliffe House,
Water Lane, Wilmslow,
Cheshire SK9 5AF

Tel: 0303 123 1113
www.ico.org.uk

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.

If you have any questions about this privacy notice, please contact data.protection@allmetal.co.uk