MidCity Place
71 High Holborn
London WC1V 6BA
Tel +44 (0)20 7061 5500
Fax +44 (0)20 7061 5620
www.triland.com

Recruitment and Employee Privacy Notice

INTRODUCTION

Triland Metals Limited ("**Triland**", "**we**", "**us**") respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data and tell you about your privacy rights and how the law protects you. Your privacy is important to us and we value the trust that you place on its safekeeping with us.

1. IMPORTANT INFORMATION AND WHO WE ARE

PURPOSE OF THIS PRIVACY NOTICE

This privacy notice gives you important information on how Triland collects and processes personal data, including any data provided through our website, when you apply for jobs at Triland, attend our events or become an employee of Triland. This privacy notice applies to applicants (including prospective applicants), employees, non-executive directors, workers (including temporary and agency workers), secondees, interns and work-experience individuals. This categorisation is for convenience and does not demonstrate any particular status.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice made available to you by us so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

CONTROLLER

Triland is the controller and responsible for your personal data. Triland's Compliance Department and Data Security Officer are responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact us using the details set out below.

CONTACT DETAILS

Company name:	Triland Metals Limited
Data Security Officer:	David Cumming
Email address:	dataprotection@triland.com
Postal address:	MidCity Place, 71 High Holborn, London WC1V 6BA, United Kingdom
Telephone number:	+44 (0)20 7061 5568

You have the right to make a complaint at any time to the Information Commissioner's Office ("**ICO**"), the United Kingdom ("**UK**") supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance wherever possible.

CHANGES TO THE PRIVACY NOTICE AND YOUR DUTY TO INFORM US OF CHANGES

This version was last updated in November 2026.

Historic versions can be obtained by contacting us.

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 relationship with us.

2. THE DATA WE COLLECT ABOUT YOU

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

In the course of the recruitment process, employment or work at Triland, we may process personal information about you and your next of kin, dependants, beneficiaries and other individuals whose personal information has been provided to us. Any references to "you" in this privacy notice, shall also refer to such next of kin, dependants, beneficiaries and other individuals (as applicable).

We may collect, process and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** includes first name, maiden name, last name, photograph, marital status, title, date of birth, gender or payroll number.
- **Employment Data** includes job title/position, place or places of work (or, in some cases, your home address and locations visited during the course of your work), employment contract, performance, appraisal and disciplinary records, training and career development records, records of any grievance procedure you have initiated (or been involved in), information on holiday/annual leave requested and taken, information on any other type of leave requested and taken (including maternity / paternity /adoption leave, parental leave, sabbaticals etc.), sickness records, other information on working activities, including, timetable, employee identification number, years of service, professional category/job title, salary level and nature of contract.
- **Background Data** includes information on professional qualifications, achievements and/or skills, for example, academic/professional qualifications, education, CV/resume, pre-employment assessment results and languages spoken. This will also include any authorisations required in respect of your work, for example, evidence that you hold a particular category of driving licence, Disclosure and Barring Service ("**DBS**") (or equivalent) checking (basic or standard (as may be applicable)) applications and responses and/or membership of a particular professional body. Other types of checks included in the employee background screening are financial (e.g. bankruptcy), electronic ID and anti-money laundering, UK digital right to work, directorships, employment references, employment gaps, worldwide sanctions and international watch lists, negative media search, social media search, FCA individual and prohibited search and WorldCheck One.
- **Contact Data** includes residential address, personal email address and telephone numbers.
- **Transaction Data** includes details about payments to and from you.
- **Technical Data** includes internet protocol ("**IP**") address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our systems and/or IT infrastructure, information relating to your devices and property, for example, your company computer and/or mobile or other device ID, mobile and direct dial phone numbers, user ID, IP addresses, log files, software and hardware inventories, cookies, information on access to Triland premises and CCTV footage.
- **Profile Data** includes your username and password, orders and transactions made by you, suitability information, your interests, preferences, feedback and survey responses.
- **Identification Data** includes your national ID/passport, details of any visa applications, driver's license, NHS number and national insurance number (or equivalent).
- **Monitoring Data** includes video, voice and text (incl. emails and instant messages) recordings.
- **Event Data** includes information relating to your attendance at events.
- **Travel Data** includes information relating to travel and accommodation undertaken / used for work purposes within and outside the UK.

- **Health and Safety Data** includes records of accidents at work, information relating to personal injury claims pursued (which have an impact on Triland), medical certificates, fitness for work assessments or other occupational health reports and drug and alcohol test results.
- **Employer Data** includes information relating to your previous and/or prospective employer.
- **Professional Data** includes any professional licences, authorisations and/or approvals, for example, registration and other information concerning regulatory approval under the rules of the Financial Conduct Authority ("**FCA**") or registrations with any other professional or regulatory body.
- **Financial Data** includes bank account details, bonuses, loans, salary, PAYE and other tax information, pension information and any other information relating to employee benefits in place from time to time.
- **Usage Data** includes information about how you use our website and applications.

We also collect, use and share **Aggregated Data** such as statistical or demographic data. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

There may be situations where we collect information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, trade union membership, information about your health, sex life, genetic data or biometric data for the purposes of unique identification and personal information relating to criminal offences and convictions ("**Special Categories of Personal Data**"). For example:

(a) we may request, on a voluntary disclosure basis, certain sensitive personal information such as information about your racial/ethnic origin, gender and health conditions which may be required to comply with anti-discrimination laws and government reporting obligations, and which we may use to help ensure equal employment opportunities;

(b) you may be required, and/or opt to provide us with information about your physical or mental health so that we can monitor absence, consider your fitness to work, consider and provide work-related accommodations or adjustments, help to process claims under any applicable insurance schemes and/or to comply with our obligations in respect of health and safety at work;

(c) we may process information relating to "live" criminal prosecutions as a part of DBS (or equivalent criminal records) checks and you may be required to provide information relating to any threatened or actual criminal proceedings or convictions to the extent that they affect your employment;

(d) you may voluntarily, upon our request or otherwise, provide other sensitive personal information to Triland (including to your colleagues / other employees or workers) in the course of your work.

Please note that processing under examples (a)-(c) each falls under Art.9(2)(b) of the United Kingdom General Data Protection Regulation and processing under example (d) falls under Art.9(2)(a) the United Kingdom General Data Protection Regulation for the purpose of additional requirements applicable to processing of Special Categories of Personal Data.

IF YOU FAIL TO PROVIDE PERSONAL DATA

Where we need to process personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are contemplating entering into with you. In this case, we may have to cancel any relationship you have with us but we will notify you if this is the case at the time.

3. HOW IS YOUR PERSONAL DATA COLLECTED?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You (or someone acting on your behalf) may give us personal data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data we are provided with in connection with:
  - entering into an employment relationship with us;
  - applying directly or indirectly (via a recruitment agency) for any vacancies with Triland;
  - subscribing to our publications;
  - requesting marketing material to be sent to you;
  - entering a competition, promotion or survey;
  - enrolling into one or more employee benefit schemes (e.g. private medical insurance);
  - signing up and/or attending our events; or
  - giving us some feedback.
- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties such as (but not limited to, background and criminal records check agencies, past and prospective employers, recruitment agencies, regulatory and government bodies, medical institutions and experts, or someone acting on your behalf.

4. HOW WE USE YOUR PERSONAL DATA

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

- Where we need to perform the contract we are about to enter into or have entered into with you.
- 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.
- Where we need to comply with a legal or regulatory obligation.
- Where there is a recognised legitimate interest.

In most cases, we do not rely on consent as a legal basis for processing your personal data. Where we do so, you have the right to withdraw your consent at any time by contacting the Data Security Officer using the contact details set out at section 1 above.

PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

We have set out below, in a table format, a description of the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

In no event does Triland sell or trade your personal data.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact the Data Security Officer if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

LAWFUL BASES AND PURPOSES FOR WHICH WE WILL USE YOUR PERSONAL DATA

Basis for processing your personal data	Type of data	Key activities
To comply with our legal and regulatory obligations, including: • The rules and regulations of the Financial Conduct Authority (FCA) and other regulatory bodies pursuant to which we: ◦ carry out background and criminal records checks and other due diligence	Identity Contact Employer	Recruitment Background screening and criminal records checks

• assess suitability and competence (incl. the fitness and propriety) of the (prospective) employee • implement measures in order to prevent market abuse and fraud • compliance with tax, health and safety and anti-discrimination or other employment laws • under judicial authorisation • for regulatory compliance or to exercise or defend the legal rights of Triland and/or any other companies in the group • report transactions and associated risks • record voice and video calls, chats and emails, where required • maintain records in connection with your role • cooperate with regulators and official enquiries or requests	Employment Background Monitoring Professional	Authorisation requests from regulators Account opening and administration of account with exchanges, trading venues and other platforms relating to your role Reporting transactions or positions to regulators, exchanges, trade repositories or similar entities Reporting to and responding to information requests from regulators, exchanges and other bodies of competent jurisdiction Provision of references
To perform a contract with you, including: • Assisting you with enquiries and requests relating to your employment at Triland • Performing our contractual obligations	Identity Identification Contact Monitoring Financial Professional Employer Employment Transaction Technical Profile Travel Event Health and Safety	Calculation and payment of salary, bonuses and other benefits Investigation of grievances Disciplinary investigation and action Performance appraisal Enrolment in and administering of membership in benefit schemes (e.g. private medical insurance and life assurance) Processing of claims

To fulfil our legitimate interest, including:
• To keep our records updated and to run our business administration
  ◦ safeguarding against loss, theft, unauthorised processing and misuse
• Improving and developing our products or services
  ◦ promoting events, our company, products and/or services
  ◦ intra-company communications
• IT and IT infrastructure development and management
  ◦ IT security, business continuity and disaster recovery
• Completion of a wider background screening for the purpose of checking that the staff's background shows no indication of bad character or lack of integrity and to protect its reputation and financial position
• Exercising and defending our legal rights
  ◦ debt recovery
  ◦ proof of evidence of authority of persons acting on behalf of our counterparties
  ◦ copyright and trademark infringement
  ◦ proof of communications, orders and transactions recorded on
	Identity
	Contact
	Transaction
	Technical
	Profile
	Usage
	Background
		Administration and operation of our business (incl. intra-group governance)
		Keeping our website and IT infrastructure updated, including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data
		Staff quality control and training
		Requesting and storing consent forms in respect of photography and videography
		Capturing, recording, using and storing photographs and videos for

instant messages, email, telephone, video calls and applications (e.g. Zoom, WeChat and Teams) ♦ Intra-group transmission ♦ CCTV		marketing purposes, in reports and other communications Establishing the facts relevant to our business (e.g. to check instructions given) Monitoring internal and external communications, orders and transactions by instant messages, email, telephone, video calls and applications (e.g. Zoom, WeChat and Teams) Background screening
Where necessary for the purposes of a recognised legitimate interest: ♦ Recording and monitoring of internal and external communications (including voice and video calls, instant messages, Zoom and Teams) for the purpose of preventing, detecting and investigating crime including money laundering, market abuse, fraud, financial crime and/or other breaches of applicable law or regulations ♦ In the instance of an emergency	Identity Contact Transaction Technical Profile Usage Health and Safety Travel Event Employment Financial Monitoring	Monitoring and review Record-keeping Reporting to exchanges and relevant authorities and/or government bodies In case of medical or other emergencies
Where explicit consent has been given: ♦ To keep our records updated and to run our business administration ♦ keep emergency contacts ♦ Providing access to or the benefit of employee benefit schemes to family members of employees	Identity Contact	Collecting, updating and storing of employees' emergency contacts Processing of personal data for the purpose of enrolment to and administration (incl. pay-out) of employee benefit schemes

CHANGE OF PURPOSE

We will only use your personal data 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 in accordance with applicable law.

If we need to use your personal data 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 data without your knowledge or consent, in compliance with the above rules, to the extent necessary and/or permitted by law.

MONITORING

Triland will carry out automated monitoring and scans of its IT and communications systems, and its mobile and other devices, through automated tools such as anti-malware software, website filtering and spam filtering. It will also carry out monitoring of its

physical premises, for example by using CCTV and access control systems. Please note that no facial recognition or biometric identification is applied to CCTV footage.

In order to comply with its regulatory obligations, Triland records and monitors all company-issued communications systems, such as telephones, voice and video calls and messaging applications (e.g. Zoom and Teams) and emails installed on work PCs, company mobile phones and iPads. Employees may also be monitored through Zoom on iPads both in the office and whilst working from home.

Triland may also carry out certain manual or partly automatic monitoring activities including, for example, email and other communications reviews, logging of browsing and activity data, remote access and wiping of devices and recording of information relating to employees' or workers' (or their devices') physical location.

PHOTOGRAPHY AND VIDEOGRAPHY

Photographs and videos of you taken in your professional capacity in the course of your employment at Triland (including headshots, material from events, promotional material etc.) may be used by Triland on the intranet, in promotional and marketing material and on the website and social media.

You may from time to time and on a voluntary basis choose to upload or provide us with your personal photographs for the purpose of their use on the staff intranet, our website or for marketing and/or promotional purposes (including social media). By sharing it with us, you acknowledge and agree that any photographs shared with Triland via Microsoft Outlook will be subject to Triland's archiving policies which may prevent permanent deletion of such emails regardless of your consent.

5. DISCLOSURES OF YOUR PERSONAL DATA

We may have to share your personal data with the parties set out below for the purposes set out in the table in section 4 above.

- Triland affiliates and their respective representatives
- Service providers who perform services on our behalf, including (but not limited to) ratings agencies, screening service providers, fraud prevention agencies and consultancy firms
- Persons and service providers acting on your behalf
- Regulatory, taxation or judicial bodies to the extent permitted by law
- Exchanges, trading venues and clearing houses
- Certain regulated professionals such as lawyers and auditors
- Potential or actual purchaser, assignee or transferee of all or part of our business

We require all third parties to respect the security and integrity of your personal data and to treat it in accordance with the law. We only permit third parties to process your personal data for specified purposes in accordance with our instructions and subject to confidentiality obligations.

6. INTERNATIONAL TRANSFERS

We may share your personal data with Triland affiliates and other external parties located outside of the UK. This will involve transferring your personal data outside the UK.

Furthermore, Triland may use cloud-based and other technologies in the provision of the services which may be located and/or hosted in data centers outside of the UK. Any transfer of personal data to such data centers shall be made in accordance with this section 6.

Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We may transfer your personal data to countries that have been approved by regulations and satisfied the data protection

test.

- Where the data protection test has not been satisfied, we may use standard data protection clauses.
- Where we use providers based in the US, we may transfer data to them pursuant to the UK-US Data Bridge, provided that they are a participating organisation under the framework and opted in to the UK extension.

7. DATA SECURITY

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

Triland implements and maintains information security practices that integrate the protection of personal data into the process lifecycles of the business.

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

8. DATA RETENTION

HOW LONG WILL YOU USE MY PERSONAL DATA FOR?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

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 and regulatory requirements. Most personal data collected is held and, where appropriate, securely deleted or destroyed in accordance with policies, guidance and rules circulated on the retention of data from time to time.

Triland's retention of your personal data is, as a general rule, 10 years, but may be shorter or longer if determined necessary and lawful by Triland from time to time.

At the end of the appropriate retention period, Triland executes secure methods of: (i) destruction of hardcopy data, which are initially stored with reference to a destruction date; and (ii) deletion of electronic records on the HR database, which can identify data that is at the end of their retention period.

9. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data. If you wish to exercise any of the rights set out below, please contact the Data Security Officer.

- **Access** | You can receive information about how we process your personal data and a copy of such personal data.
- **Rectification** | You can require us to correct your personal data, where you consider it to be inaccurate or incomplete.
- **Erasure** | You can require the deletion of your personal data, to the extent permitted by law.
- **Restriction** | You can request the restriction of the processing of your personal data.
- **Objection** | You may object to the processing of your personal data where Triland has relied on legitimate interest and/or recognised legitimate interest as its lawful basis for such processing.
- **Transfer** | Where legally applicable, you can require us to transfer (or have returned) your personal data where technically

feasible.

- **Consent withdrawal** | You have the right to withdraw your consent at any time.

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 your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

TIME LIMIT TO RESPOND

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

UPDATES TO THIS NOTICE

This notice may be updated periodically to reflect any necessary changes in our privacy practices. You have a responsibility to ensure that you regularly review this notice but where such changes will materially affect your privacy rights, we will inform you by circulating a Company-wide email and indicate at the top of the notice when it was most recently reviewed.