Trident Lifting Solutions

Policy Statement - Trident Lifting Solutions Limited (“Trident”, “the Company”)

Trident Lifting Solutions Limited is committed to high standards of professional conduct, integrity and accountability. As a specialist lifting and crane solutions provider operating in safety-critical environments, we recognise that the behaviour and standards of our people are fundamental to building a strong, respectful culture and protecting our reputation as a trusted industry leader.

We expect everyone working for or on behalf of the Company to act with professionalism, respect and responsibility at all times, reflecting our values and supporting a positive working environment. Clear standards of behaviour are essential to ensure safety, quality and effective collaboration across our projects and teams.

1. Purpose

This policy sets out how Trident Lifting Solutions Limited ("Trident", "the Company") handles requests to access personal data. It covers:
formal data subject access requests ("DSARs" or "SARs") under UK data protection law;
informal requests by workers to see information held on their personnel file;
requests made by a representative on behalf of a data subject;
requests from third parties, including the police, regulators, courts, insurers and other employers; and
how Trident will search, review, disclose, withhold or redact information in a lawful, consistent and auditable way.
The policy is designed to protect individuals' rights while allowing Trident to meet its legal duties, run the business, investigate issues, and protect the rights of other people whose data may sit in the same records.
This policy does not give managers a right to browse another worker's mailbox, device or personal file out of curiosity. Mailbox access is governed by the Access to Employee Email Accounts Policy (HR-POL-076). Monitoring is governed by the Employee Monitoring Policy. Both remain subject to UK GDPR.

2. Scope

This policy applies to all personal data processed by Trident, whether held electronically or in paper form, including data held in HR systems, payroll, SAGE, email, shared drives, project systems, CCTV where applicable, occupancy or access-control records, and records held by processors acting for Trident.
It applies to requests from:
current and former employees;
workers, agency staff, contractors, consultants, directors and applicants;
clients, suppliers and other individuals whose personal data Trident processes; and
a parent, attorney, solicitor or other representative acting with valid authority.
It applies across Trident and any associated company that uses Trident systems or HR support, unless a group company publishes its own access procedure.

3. Legal framework

Trident will handle access requests in line with:
UK GDPR (as amended);
the Data Protection Act 2018;
the Data (Use and Access) Act 2025 ("DUAA"), including rules on proportional searches, stop-the-clock mechanisms and identity verification;
the Privacy and Electronic Communications Regulations 2003 (as amended), where relevant;
ICO guidance on the right of access; and
the Access to Medical Reports Act 1988 where a request concerns a report from the individual's GP or treating clinician.
Where this policy and the statute differ, the statutory position prevails.

4. Definitions

Personal data: information relating to an identified or identifiable living individual.
Special category data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data for identification, health data, or data concerning a person's sex life or sexual orientation.
Data subject: the individual the personal data is about.
Controller: Trident, which determines the purposes and means of processing.
Processor: a third party that processes personal data on Trident's behalf.
DSAR / SAR: a request by a data subject, or someone acting for them, to obtain confirmation that Trident processes their data, a copy of that data, and the supplementary information required by UK GDPR Articles 13 to 15.
Personnel file: the HR and payroll records Trident keeps about a worker, including contract, pay, absence, performance, training and, where held, disciplinary or grievance papers.
Third-party data: personal data about someone other than the requester that appears in the same document or mailbox.

5. Principles

When dealing with any access request Trident will:
treat the requester fairly and without unlawful discrimination;
verify identity before releasing personal data;
search only what is necessary and proportionate to the request;
disclose the requester's own personal data unless an exemption applies;
protect third-party personal data, confidential information and legally privileged material;
meet statutory timescales, or record why an extension or stop-the-clock pause applies;
keep an audit trail of the request, searches, decisions and disclosure; and
not use an access request as a reason to delete or alter records that should be retained, except to correct inaccurate data through the normal process.

6. Informal access to a personnel file

Workers may ask HR or their line manager to see factual information held on their own personnel file without making a formal DSAR. Typical informal access includes:

a copy of the contract, job description or variation letters;
pay, tax code and pension contribution summaries already available through payroll;
training and competence records;
holiday and absence balances; and
a copy of a warning, appeal outcome or performance review that was already issued to the worker.
Informal requests should be made in writing to HR (email is acceptable). HR will usually respond within 10 working days where the information is readily available and does not require a wide search of email or project systems.
Informal access is not a substitute for a DSAR. If the worker wants a full search of email, devices, CCTV or unstructured records, or if the request is complex, HR will treat it as a DSAR and follow sections 7 to 14.
Managers must not hand over another person's file, medical report, investigation bundle or mailbox contents under an "informal" request. Those disclosures need HR (and, where relevant, the Data Protection Lead) to review exemptions and third-party data.

7. The right of access (formal DSAR)

A data subject is entitled to:
confirmation of whether Trident processes their personal data;
a copy of that personal data; and
supplementary information, including the purposes of processing, the categories of data, the recipients or categories of recipient, retention periods or the criteria used to set them, the source of the data if it was not collected from the individual, information about automated decision-making where relevant, and information about their other data-protection rights.
The right is to the individual's personal data, not to every document in which their name appears. Trident may extract the personal data or provide copies of documents with third-party information redacted. Trident is not required to create new documents or to provide legal advice about the meaning of the records.

8. How to make a DSAR

8.1 Who can make the request

A request may be made by:
the data subject;
a solicitor, union representative or other agent with written authority;
a person with lasting power of attorney or a court-appointed deputy covering property and affairs or relevant personal welfare decisions; or
a parent or guardian of a child, where it is reasonable to treat the parent as acting for the child. Competence and the child's best interests will be considered. A child who understands the request may make or object to it themselves.

8.2 Where to send it

Requests should be sent in writing to HR, marked "Data subject access request". Email is acceptable. A verbal request is still valid. If a request is made verbally, the receiving manager must record the date, the requester's name, what is asked for, and pass it to HR the same working day.
Workers should not send DSARs to a personal mailbox and assume they have been received. HR will acknowledge valid requests.

8.3 What to include

To help Trident find the right information without delay, the requester should include:

full name, date of birth and contact details;
payroll number, employee number or role and work location, if they work or worked for Trident;
the relationship with Trident (employee, leaver, applicant, contractor, client contact);
the information sought, including date ranges, systems, sites, managers or topics if known;
whether the request is limited to the personnel file or also covers email, devices or other systems;
proof of identity (see section 9); and
if acting for someone else, proof of authority.
A requester does not have to use the words "subject access request" or complete a form. If it is reasonably clear that they want their personal data, HR will treat it as a DSAR.

9. Identity and authority checks

Trident will not release personal data until it is satisfied about the requester's identity and, where relevant, their authority to act.
Typical evidence includes a copy of a passport or driving licence plus a recent utility bill or bank statement, or an in-person check against records already held. For current workers, HR may verify identity through existing HR records and a work email confirmation where that is proportionate.
If the request comes from a solicitor or other representative, Trident will ask for a signed letter of authority dated within the last three months, or other evidence that the representative is instructed. Trident may contact the data subject directly to confirm the instruction.
If identity or authority cannot be verified, Trident may refuse to proceed until it is. The statutory time limit does not start until Trident has the information reasonably required to confirm identity.

10. Clarifying and scoping the request

If a request is broad (for example "everything you hold about me"), Trident may ask the requester to narrow it by date range, system, site, manager or topic. Under the DUAA and ICO guidance Trident may pause the response clock ("stop the clock") while it waits for clarification that is reasonably needed to find the data.
Trident will not insist on narrowing as a condition of starting work. If the requester declines to limit the request, Trident will carry out a reasonable and proportionate search of the systems and locations where the data is likely to be held, and will explain the scope of that search.
A request is not invalid because it is made during a grievance, disciplinary, tribunal claim or exit process. Those processes continue in parallel. Investigation materials will still be reviewed against the exemptions in section 13.

11. Timescales

Trident will acknowledge a DSAR promptly and usually within five working days of receipt by HR.
The statutory deadline is one calendar month from the later of: receipt of the request, confirmation of identity, or receipt of any clarification reasonably required to locate the data.
For complex or multiple requests Trident may extend the deadline by up to two further months. HR will tell the requester within the first month that an extension applies and why.
"Stop the clock" pauses for identity or necessary clarification are recorded on the case file. The clock restarts when the information is received.
If a large volume of material has to be reviewed for third-party data or privilege, HR will give an update rather than missing the deadline in silence.
Informal personnel-file requests remain subject to the 10 working day target in section 6 unless they are converted to a DSAR.

12. Fees

A DSAR is free of charge in almost every case.

Trident may charge a reasonable fee, or refuse to act, only where a request is manifestly unfounded or excessive, including where it repeats a recent request without a good reason. Any fee will reflect administrative cost only. HR will explain the decision in writing and tell the requester they can complain to Trident or the ICO.

Trident will not charge for providing a contract, payslip, holiday record or similar document that the worker is entitled to see as part of ordinary employment administration.

13. Searches and review

13.1 Reasonable and proportionate searches

HR, with IT where needed, will identify the systems likely to hold the data. A typical worker DSAR search may include:

the HR information system and personnel file;

payroll and SAGE records;

training and competence records;

occupational health reports that Trident is entitled to hold;

relevant shared drives or project folders named in the request;

the worker's own work mailbox and, where justified by the request, other mailboxes or Teams/SharePoint locations identified by keyword, date range and correspondent; and

CCTV or access-control logs only where the requester specifies a time, place and reason, and the footage is still retained.

Trident is not required to search every backup tape, every colleague mailbox, or archived systems that cannot reasonably be accessed. The search plan will be recorded.

13.2 Review before disclosure

Every item in scope will be reviewed before release. Reviewers will identify:

the requester's personal data, which will normally be disclosed;

third-party personal data, which will be redacted unless the other person consents or it is reasonable to disclose without consent;

special category data, which will be disclosed only where it is the requester's own data or another lawful basis and exemption assessment allows it;

legally privileged advice;

management forecasting, negotiation or investigation material covered by an exemption; and

information that would prejudice crime prevention, regulatory action or someone's rights and freedoms.

Redactions will be visible as redactions, not silent deletions, unless showing the existence of the material would itself cause the harm the exemption is designed to prevent.

14. Exemptions and withholding

Trident will rely on exemptions in the Data Protection Act 2018 and associated schedules only where they apply. Common examples in an employment setting include:

confidential employment references given by Trident;

information about management forecasting or planning that would prejudice the business if disclosed at that time;

records of negotiations with the requester that would prejudice those negotiations;

legal advice and litigation privilege;
information that would identify another individual who has not consented, where it is not reasonable to disclose without consent;
information that would prejudice the prevention or detection of crime, or an ongoing investigation, if disclosed at that time;
exam scripts or professional-test questions where a statutory exemption applies; and
occupational health or medical reports obtained under the Access to Medical Reports Act 1988 where the individual has not yet exercised their rights against the clinician, or where disclosure is otherwise restricted.
Where an exemption applies to part of a document, Trident will disclose the rest. Where Trident withholds information it will, so far as the exemption allows, tell the requester that material has been withheld and which exemption is relied on. Trident will not describe withheld material in a way that defeats the exemption.

15. How information will be provided

Trident will usually provide the response by secure email to an address the requester has confirmed, or through another secure file-transfer method for large files. Paper copies can be provided on request.
The response pack will normally include:
a covering letter confirming that a search has been completed, the systems searched, the date range and any limitations;
the personal data, with redactions applied;
the Article 15 supplementary information, or a pointer to the current Employee Privacy Notice where that notice already supplies it; and
an explanation of any exemption, extension or refusal.
Trident may provide data in a commonly used electronic form. It is not obliged to restore deleted items that are no longer reasonably accessible, or to produce data in a requester's preferred software format if a reasonable alternative is offered.

16. Third-party requests (not made by the data subject)

Requests from someone who is not the data subject, and who does not have the data subject's authority, are not DSARs. They will be considered separately.

16.1 Police, courts and regulators

Trident may disclose personal data without the individual's consent where required by law or where a relevant exemption applies, for example a court order, a statutory notice, or a formal request from the police or a regulator that meets the tests in the Data Protection Act 2018. HR or the Data Protection Lead must review the request, the legal basis and the minimum data needed. Disclosures will be recorded.

16.2 Other employers and reference requests

Employment references are handled under the Reference Requests Policy. A reference request is not a DSAR. A worker who wants to see a reference Trident has given may make a DSAR, but confidential references given by Trident are generally exempt.

16.3 Family members, colleagues and informal askers

Trident will not disclose a worker's personal data to a spouse, relative, colleague or manager who simply asks for it, unless the worker has consented, the disclosure is a necessary employment function (for example payroll or next-of-kin in an emergency), or another lawful basis applies.

17. Medical and occupational health information

Health information is special category data. Access is limited to people who need it to manage fitness for work, adjustments, statutory sick pay or legal duties.

A worker may request a copy of occupational health reports that Trident holds. Where the report was obtained from the worker's own GP or treating clinician, the Access to Medical Reports Act 1988 may give the worker additional rights against that clinician. Trident will not obtain a GP report without written consent.

Managers will not normally be given the underlying clinical detail. They will receive fitness-for-work conclusions, restrictions and recommended adjustments only.

18. Email, devices and monitoring data

A DSAR may include personal data in work email, Teams messages, device logs or monitoring records. That does not mean the requester is entitled to another person's mailbox or to a complete dump of a shared inbox.

Mailbox access for business continuity, investigation or handover is a different process and must follow the Access to Employee Email Accounts Policy. IT must not fulfil a DSAR by granting the requester live access to systems they are not authorised to use.

Personal data generated by monitoring (for example building access logs, vehicle trackers on company vehicles, or IT logs) may be in scope if it relates to the requester and is still retained. Trident will disclose it in accordance with the Employee Monitoring Policy, the Privacy Notice and the exemptions above.

19. Correcting, restricting or deleting data

The right of access sits alongside other rights, including rectification, erasure, restriction, objection and data portability. Those rights are not automatic in every employment record.

If a DSAR shows that data is inaccurate, HR will correct it. If the requester wants information deleted, HR will consider the request against Trident's retention needs, legal obligations and the Records Retention Schedule. Investigation, payroll, tax, health and safety and limitation-period records will often have to be kept.

Requests to correct or delete data should be made in writing to HR and will be handled under the Data Protection Policy.

20. Roles and responsibilities

HR: owns this policy, logs DSARs, verifies identity, coordinates searches, applies exemptions with advice, issues the response and keeps the case file.

Data Protection Lead / DPO (if appointed): advises on complex, high-risk or disputed requests, large email searches, special category data and whether to extend or refuse.

IT: runs agreed technical searches, exports data securely, and does not grant informal mailbox access in place of a DSAR review.

Line managers: pass any access request to HR the same working day, do not withhold or destroy records, and do not disclose other people's data.

Employees and workers: use official channels, provide identity and enough detail to find the data, and do not remove or copy Trident records without authority.

Processors and suppliers: must support Trident DSARs in line with their contract and must not respond directly to a data subject unless Trident instructs them to.

21. Record-keeping

HR will keep a DSAR register recording the requester, date received, identity checks, scope, systems searched, exemptions used, date of response, extensions and any complaint. Case files will be retained in line with the Records Retention Schedule and the Data Protection Policy.
Search terms, mailboxes reviewed and reviewer names will be recorded so that Trident can show a reasonable search if the ICO or a court asks.

22. Complaints

If a requester is unhappy with the scope, redactions, timing or completeness of a response they should write to HR within 21 days, explaining why. HR will review the file, involving the Data Protection Lead where appropriate, and reply in writing.
A requester may also complain to the Information Commissioner's Office (ico.org.uk) or seek a court order. Trident will cooperate with any ICO case.
Using this policy in good faith will not lead to detriment. Knowingly making a false request, or using disclosed data to harass another person, may be treated as a disciplinary matter.

23. Security of disclosed information

Response packs contain personal data and sometimes special category data. They must be sent only to the verified requester, using a work email already on file, a confirmed personal email, or a password-protected file with the password sent separately. Packs must not be forwarded to a manager "for interest". Recipients are responsible for storing their copy securely.

24. Related policies and documents

HR-POL-006 Data Protection, GDPR and Cyber Security Policy;
HR-POL-076 Access to Employee Email Accounts Policy;
Employee Privacy Notice;
Employee Monitoring Policy;
Reference Requests Policy;
Records Retention Schedule;
Disciplinary Policy and Grievance Policy;
Sickness Absence and Medical Capability Policy; and
IT and Acceptable Use policies.

25. Review

This policy is non-contractual and may be amended by Trident. It will be reviewed at least annually, or earlier if the ICO issues new guidance, the DUAA or UK GDPR is amended, or Trident's systems for holding HR data change. The statutory position prevails if the law changes before this policy is updated.

AUTHORISED AND SIGNED

SIGNED

Chris Conway
Director

Review: **Annually**
Date: **28/08/2026**
Next Review: **28/08/2027**

SIGNED

Martina Oyite
Chief People Officer

Review: **Annually**
Date: **28/08/2026**
Next Review: **28/08/2027**