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

The purpose of this policy is to establish clear guidelines and procedures for the secure destruction of media containing sensitive or confidential information within Trident. This policy ensures compliance with data protection regulations, such as GDPR, and mitigates the risk of unauthorised access, data breaches or misuse of confidential data.

2. Scope

This policy applies to all workers, contractors and third-party vendors involved in handling, storing, or destroying media containing sensitive, confidential, or personal data at Trident. It covers all types of media, including but not limited to:

- Hard drives (HDDs/SSDs)
- USB drives
- CDs, DVDs, and Blu-rays
- Mobile devices (smartphones, tablets)
- Printed documents and files
- Any other electronic or physical media containing data

3. Definitions

- **Media:** Any physical or electronic storage device used to store information, such as hard drives, tapes, and USBs, as well as physical documentation.
- **Sensitive Data:** Data that includes personal, financial, intellectual property, or other confidential information that requires secure handling and destruction.
- **Destruction:** The irreversible removal or obliteration of data from media, ensuring that it cannot be recovered or reconstructed.

4. Destruction Methods

To ensure data security, the following destruction methods must be used based on the type of media:

a. Electronic Media

- **Hard drives (HDDs/SSDs):** Use degaussing (erasing magnetic fields) or physical destruction through shredding, crushing, or disassembly to render the device inoperable and unrecoverable.
- **USB drives and other removable media:** Use secure erasure methods (multiple overwriting cycles) or physical destruction through shredding.
- **Optical media (CDs, DVDs, Blu-rays):** Shred or cut into small, unreadable pieces.
- **Mobile devices (smartphones, tablets):** Perform secure data wiping and reset to factory settings. If possible, physically destroy the device.

b. Physical Media

- **Paper documents:** Use cross-cut shredders that ensure the paper is reduced to small particles. If outsourced, use certified document destruction services.

5. Destruction Procedures

All media must be securely destroyed as per the following procedures:

a. Inventory and Authorisation

- All media slated for destruction must be logged in an inventory that includes asset tags, serial numbers, or other identifying information. Authorization must be obtained from the line manager or the IT security team before destruction.

b. Destruction

- Authorized personnel or approved third-party vendors are responsible for the destruction of media. When using third-party vendors, ensure that they are certified for secure media destruction.

c. Documentation

- Upon destruction, a Certificate of Destruction or equivalent proof of destruction must be provided and stored in compliance with company data retention policies. This certificate must include the date, method, and type of media destroyed.

6. Third-Party Vendors

If third-party vendors are used for media destruction, Trident will:

- Only work with certified destruction vendors compliant with GDPR and other relevant standards.
- Ensure third-party vendors provide a Certificate of Destruction and comply with Trident's security standards.
- Include media destruction clauses in vendor contracts to safeguard data security.

7. Employee Responsibilities

- Employees must follow this policy when disposing of any media containing sensitive or confidential data.

- All data must be wiped or securely erased before media is sent for physical destruction.
- Under no circumstances should sensitive or confidential information be disposed of in general waste.
- Employees must report any issues with media destruction to their line manager or IT security.

8. Training and Awareness

Trident will provide regular training to all employees to ensure compliance with the Media Destruction Policy. This will include awareness of the importance of secure media destruction and how to follow the appropriate procedures.

9. Compliance and Auditing

- The IT security team will conduct regular audits to ensure compliance with this policy.
- Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

10. Exceptions

Any exceptions to this policy must be documented and approved by the IT security team and senior management.

11. Review

This policy will be reviewed annually or in response to any regulatory or technological changes that impact Trident's data security or destruction procedures.

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**