

Annex D – E-Waste & Disposal Policy

Attached to the Digissential Master Legal Policies & Terms (South Africa)

Effective date: 2025-08-14

1. Purpose & Legal Basis

1.1 This Annex sets out Digissential's policy for the lawful, safe and environmentally responsible handling, storage, transport and disposal of electronic waste ("e-waste") generated through our operations and client services.

1.2 This policy aligns with applicable South African law and guidance, including the National Environmental Management: Waste Act, 2008 (NEM:WA) and associated regulations; Extended Producer Responsibility (EPR) requirements for electrical and electronic equipment; the Occupational Health and Safety Act (OHSA); and the Protection of Personal Information Act (POPIA) for data-bearing devices. Where stricter legal requirements apply, they prevail.

1.3 This Annex must be read with the Master Legal Policies (including Annex B – Privacy & POPIA; Annex C – Warranty & Returns; Annex E – On-Site Safety) and Annex A (fees).

2. Scope

2.1 Applies to all devices, components, consumables and media we accept, store, refurbish, recycle or dispose of, including but not limited to: laptops, desktops, servers, components (RAM, SSD/HDD, GPUs, motherboards), mobile phones/tablets, peripherals (keyboards, mice, printers, routers), monitors/TVs, cables, power supplies, and data-bearing media (HDDs, SSDs, memory cards).

2.2 Includes hazardous sub-components requiring specialised handling: batteries (especially lithium-ion), capacitors, lamps, and other items subject to hazardous-waste controls.

3. Definitions

- 3.1 "EEE/WEEE" – electrical and electronic equipment / waste electrical and electronic equipment.
- 3.2 "Data-bearing device" – a device or medium capable of storing Personal Information (e.g., HDDs, SSDs, phones, memory cards).
- 3.3 "Reuse/Refurbish/Repair" – extending useful life through cleaning, testing, and component replacement without changing core function.
- 3.4 "Recycle" – processing materials into secondary raw materials via an approved recycler.

- 3.5 “Disposal” – final treatment: recycling, recovery, or destruction at a licensed facility; landfill only where legally permitted and as a last resort.
- 3.6 “Approved recycler/contractor” – a licensed service provider meeting NEM:WA requirements for handling, transport and treatment of e-waste.
- 3.7 “Chain-of-custody record” – documentation tracing custody from intake to final treatment (receipts, manifests, certificates of destruction/recycling).
- 3.8 “Thermal runaway” – uncontrolled battery heating reaction that may cause fire or venting.
- 3.9 “Certificate of Data Destruction (CoDD)” – written confirmation that data sanitisation/destruction was completed, including method(s) used and device identifiers.

4. Roles & Responsibilities

- 4.1 Digissential operates as a repair/refurbishment service and e-waste collector for items arising from our services; we do not dispose via informal channels or unlawful dumping.
- 4.2 Where EPR obligations apply (e.g., if acting as a “producer/importer” of covered equipment), Digissential will register or align with a Producer Responsibility Organisation (PRO) and comply with reporting duties.
- 4.3 Staff follow this policy, complete required training and use appropriate PPE. Supervisors ensure compliance, record-keeping and vendor due diligence.
- 4.4 Only approved, licensed contractors and transporters may be used for recycling, recovery or final disposal.

5. Waste Hierarchy & Circular Economy

1. 5.1 Prevent: avoid waste generation by prioritising repair and parts harvesting where safe and economical; proactively advise clients on repair vs. replacement benefits.
2. 5.2 Reuse/Refurbish: prioritise refurbishment and reuse (with client consent) including internal refurbishment and resale/donation programmes.
3. 5.3 Recycle: route end-of-life items to approved recyclers to recover materials and avoid landfill.
4. 5.4 Dispose: use destruction/final disposal only where reuse/recycling is not reasonably practicable or lawful.

6. Client Communication & Transparency

- 6.1 Provide clients with plain-language explanations of e-waste options, environmental impacts, and the benefits of repair and reuse.
- 6.2 Offer a standardised Data Destruction Confirmation slip for all jobs with data-bearing devices; CoDD available upon request.
- 6.3 Publish/attach a clear, itemised fee schedule for optional services (e.g., certified data destruction, battery disposal) linked to Annex A.

- 6.4 Align messaging with “Right to Repair” principles and consumer education on device longevity and e-waste reduction.

7. Acceptance, Intake & Ownership

- 7.1 Verify rightful ownership or lawful authority to surrender devices (see intake procedures and Second-Hand Goods compliance).
- 7.2 Record client instructions on intake/handover form: return, reuse, donate, recycle, or destroy. Absent instruction, default to secure retention while seeking confirmation.
- 7.3 Unacceptable without prior arrangement: biohazard-contaminated equipment, devices containing free liquids or severe chemical contamination, and items prohibited by law.
- 7.4 Abandoned devices are processed per the Master Legal Policies (Device Collection & Abandonment) with priority to secure data destruction and lawful disposal.

8. Data Sanitisation & Security (POPIA & NIST SP 800-88)

8.1 Sanitisation Standards: For data-bearing devices, apply NIST SP 800-88 Rev.1 methods appropriate to media type, with verification:

- • Magnetic HDDs: Clear (single/multi-pass overwrite) or Purge (degauss), or Destroy (shred).
- • SSDs/Flash (incl. NVMe/SATA): Manufacturer Sanitize/Secure Erase, Cryptographic Erase, or Destroy (disintegrate/shred) where erase cannot be verified.
- • Mobile devices: Full factory reset plus secure wipe; remove accounts/MDM; where encryption is enabled, crypto-erase acceptable.
- 8.2 Verification: Capture tool logs/screenshots or checksum reports where available; perform random sampling verification for batches.
- 8.3 Chain-of-Custody: Record device identifiers (make/model/serial/IMEI), sanitisation method, operator, date/time, and verification outcome; issue CoDD upon request.
- 8.4 POPIA: Limit access to Personal Information to what is strictly necessary; store records securely; follow Annex B for retention and breach notification duties.

9. Storage, Segregation & Labelling

- 9.1 Store e-waste in a secure, dry area, segregated by stream: reusable stock; data-bearing devices pending sanitisation; hazardous sub-components (e.g., batteries); mixed e-waste awaiting collection.
- 9.2 Label containers with content, hazard (where applicable) and intake date. Damaged lithium-ion batteries are isolated in non-conductive containment with heightened precautions.
- 9.3 Keep on-site storage periods reasonable; schedule periodic collections by approved contractors to prevent accumulation.

10. Batteries & Hazardous Sub-Components

- 10.1 Storage: Use fire-resistant, non-conductive containers; maintain cool, dry conditions (indicative target 5–30°C) away from ignition sources; segregate damaged or swollen cells immediately.
- 10.2 Handling: Avoid puncture, crushing, or short-circuit; cover terminals during transport; never discard in general waste.
- 10.3 Response: Keep sand/vermiculite and appropriate fire extinguisher accessible; DO NOT use water on lithium battery fires.
- 10.4 Hazard Streams: Route batteries, lamps and capacitors via licensed hazardous-waste handlers. Manage spills/leaks per Annex E (On-Site Safety).

11. Transport, Export & Compliance

- 11.1 Engage only licensed transporters; maintain due-diligence records (licences, certifications, insurance).
- 11.2 Accompany each outbound consignment with documentation noting quantities, categories, hazards and destination.
- 11.3 Obtain and retain Certificates of Recycling/Recovery/Destruction; archive weighbridge slips or material recovery reports where applicable.
- 11.4 Do not export e-waste except in full compliance with applicable laws and international obligations. For air shipments of lithium batteries or devices containing them, comply with IATA Dangerous Goods Regulations and UN 38.3 where applicable.

12. Approved Recycler Due Diligence & Contracts

- 12.1 Certifications: Prefer recyclers with eWASA, R2v3, or e-Stewards certification (or equivalent recognised standard).
- 12.2 Audits: Perform annual desktop reviews; conduct on-site audits for high-volume partners where feasible.
- 12.3 Contractual Clauses: Prohibit downstream export to non-compliant jurisdictions; require transparent downstream tracking; mandate data protection for any residual data; grant Digisential audit/inspection rights; define corrective actions and termination for non-compliance.

13. Records: E-Waste Register & Retention

- 13.1 Maintain an E-waste Register capturing: intake date; client/job reference; consent/instruction; device description and serial/IMEI; specific hazardous components; weight per device/batch; sanitisation method and verification reference; outbound date; transporter/recycler details; certificate IDs; and chain-of-custody links.
- 13.2 Digital Record-Keeping: Use searchable digital logs with backup; restrict access per role.
- 13.3 Retention: Retain records for at least three (3) years (or longer where legally required); where Personal Information is included, apply POPIA minimality and security controls.

14. SOPs, Training & Drills

- 14.1 SOPs: Maintain detailed, step-by-step procedures for intake, storage, sanitisation, battery handling, transport documentation and incident response.
- 14.2 Training: Provide induction and annual refreshers on e-waste handling, NIST 800-88 methods, POPIA, battery safety, and chain-of-custody.
- 14.3 Drills: Conduct quarterly drills covering lithium battery thermal events and spill response; document outcomes and improvements.

15. Incident Response & Escalation

- 15.1 Immediate Actions (RESCUE → CONFINE → REPORT → SECURE → CLEANUP): attend to life safety; isolate area; notify supervisor; secure waste; initiate clean-up using appropriate materials/PPE.
- 15.2 Escalation: Trigger internal escalation matrix for fires, hazardous spills, injuries, or suspected unlawful disposal; consider notifications to the competent environmental authority per legal thresholds.
- 15.3 Data Incidents: If Personal Information is compromised, follow Annex B (POPIA) breach notification to affected data subjects and the Information Regulator.
- 15.4 Post-Incident Review: Complete incident report and root-cause analysis within ten (10) Business Days; implement corrective and preventive actions.

16. Audits, Performance & Improvement

- 16.1 Internal Audits: Conduct semi-annual audits covering storage, labelling, documentation, vendor compliance and training currency.
- 16.2 Vendor Reviews: Review approved recyclers/transporters at least annually for licensing, performance and compliance status.
- 16.3 Metrics: Track volumes (by weight), reuse vs. recycle rate, incident rate, training completion; use metrics to drive continuous improvement.

17. Fees & Consumer Terms

- 17.1 Any handling or disposal fees are disclosed upfront and reflected in Annex A (Standard Fees & Diagnostic Rates).
- 17.2 Consumer rights under the CPA are not limited by this Annex.

18. Updates, Versioning & Contact

- 18.1 This Annex may be updated to reflect changes in law or practice. Material changes will be recorded in Annex F (Change Log).
- 18.2 Contact: digissentialteam@gmail.com

Appendix A – Data Sanitisation Methods (Summary)

- A1. HDD: Overwrite (1–3 passes) with verify; degauss (where available) for purge; shred for destruction.
- A2. SSD/NVMe/Flash: Manufacturer Sanitize/Secure Erase or cryptographic erase with verification; physical destruction if verification fails.
- A3. Mobile: Factory reset + secure wipe; account/MDM removal; crypto-erase if encrypted.

Appendix B – Spill & Thermal Event Response (Quick Guide)

- B1. RESCUE: Move people to safety; call emergency services if required.
- B2. CONFINE: Isolate area; disconnect power where safe; prevent spread.
- B3. REPORT: Notify supervisor and log incident; initiate escalation matrix.
- B4. SECURE: Use sand/vermiculite; avoid water on lithium battery fires; ventilate.
- B5. CLEANUP: Use appropriate PPE and containers; dispose via licensed hazardous-waste contractor; document and certify.

Appendix C – Recycler Due Diligence Checklist

- C1. Valid licences/permits; insurance; EPR alignment.
- C2. Certifications (eWASA/R2v3/e-Stewards or equivalent) current and in good standing.
- C3. Process flow transparency; downstream partners identified and compliant.
- C4. Data handling controls; secure zones; media destruction capabilities.
- C5. Environmental, health and safety performance records; incident history.
- C6. Contract clauses: no informal export; audit rights; corrective action terms.