20-Point Office IT Clear-Out & Data Security Checklist

Tick each item when completed. Record exceptions and assign follow-up actions.

Organisation: _____ Date: _____

01 Asset identification

- ☐ 01. Create an inventory of computers, laptops, servers, phones and other IT assets.
- ☐ 02. Record asset tags, serial numbers, locations and assigned owners.
- ☐ 03. Identify leased, shared or third-party devices and obtain disposal approval.
- ☐ 04. Flag all data-bearing devices, including loose drives and removable media.

02 Data security and sanitisation

- ☐ 05. Confirm retention requirements and back up records that must be kept.
- ☐ 06. Obtain authorisation before erasing data; check for legal or investigation holds.
- ☐ 07. Remove accounts, access tokens and device-management locks where appropriate.
- ☐ 08. Agree a verified sanitisation or physical destruction method; log any failures.

03 Segregation and reuse

- ☐ 09. Separate reusable equipment from damaged or end-of-life items.
- ☐ 10. Keep unsanitised devices in a secure, access-controlled area.
- ☐ 11. Separate loose batteries and flag swollen or damaged batteries for specialist advice.
- ☐ 12. Group equipment by type; keep accessories with reusable devices where practical.

Practical planning aid; not a substitute for your organisation’s compliance procedures.

20-Point Office IT Clear-Out & Data Security Checklist

Tick each item when completed. Record exceptions and assign follow-up actions.

Organisation: _____ Date: _____

04 Collection preparation

- ☐ 13. Confirm quantities, collection address, access restrictions and loading arrangements.
- ☐ 14. Agree accepted items, packaging requirements and any applicable charges.
- ☐ 15. Pack equipment securely and label containers without exposing sensitive data.
- ☐ 16. Nominate a handover contact and reconcile items against the collection inventory.

05 Documentation and closure

- ☐ 17. Obtain the appropriate waste transfer or consignment documentation, where required.
- ☐ 18. Request data sanitisation or destruction evidence for relevant assets.
- ☐ 19. Reconcile collected items and certificates with the original asset inventory.
- ☐ 20. Retain records securely, update the asset register and resolve any discrepancies.

Exceptions / follow-up actions

Reviewed by: _____ Date: _____

Need help with your office IT clear-out?

Contact T&M Reuse for collection and secure IT recycling support.

Practical planning aid; not a substitute for your organisation’s compliance procedures.