Secure Disposal of IT Equipment

# Secure Disposal of IT Equipment

The Ministry of Justice (MoJ) and its Executive Agencies and Arms Length Bodies use a wide variety of equipment, including desktop computers, laptops, USB memory sticks and other mobile devices. This equipment is procured and managed though MoJ suppliers, who are normally responsible for the secure disposal of the equipment when it is no longer used. Typically, a supplier managed device will have a supplier asset tag on it, making it easier to identify who to ask for help with disposal.

However, there are also other devices across the MoJ estate which might have been procured and managed locally. It is crucial that they are disposed of in a secure manner, to prevent data being leaked.

To determine the correct disposal requirement, use the following table to identify the correct outcome, depending on the type of equipment and its security classification. If the table does not cover your exact requirement, contact the Operational Security Team: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)

Note: When disposing of SECRET or TOP SECRET equipment or materials, always contact the Operational Security Team: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)

|  |  |  |
| --- | --- | --- |
| Equipment or asset type | Data deletion method | Disposal method |
| Flash (USB), Memory cards, and Solid State Drives (SSD) | Delete the data, or erase using manufacturer instructions. | Destroy using commercially available disintegration equipment, to produce particles of a maximum of 6 mm in any direction. |
| Hard disk | Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back. | Break the platters into at least 4 pieces. This can be done either manually or by using a commercially available destruction product suitable for use with hard disks. Alternatively, apply a Lower Level degauss and then apply a destructive procedure that prevents the disk from turning. For example, punch holes into the platters, or twist or bend them. |
| Optical media | Data deletion is not possible. See also the note following this table. | Shred or disintegrate using equipment that meets a recognised international destruction standard. Particles should be no larger than 6 mm in any direction. A high capacity CD and DVD shredder is available at 102 Petty France, suitable for items up to TOP SECRET. Contact [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk) for help with this option. |
| Magnetic tapes and floppy disks | Overwrite the entire storage space with random or garbage data, verifying that only the data used to perform the overwrite can be read back. | Destroy using a commercially available shredder that meets a recognised international destruction standard. Particles of tape should be no larger than 6 x 15 mm. Alternatively, apply a Lower Level degauss and then cut the tape to no larger than 20 mm in any direction. |

Note: Theoretically, data deletion is possible on some RW-capable media. For simplicity, however, the safer assumption is that rewriting and therefore data deletion is not possible on optical media.

Owners of the data storage devices are responsible for procuring services that meet the necessary destruction outcomes as described above. Assurance shall be required that the appropriate destruction has taken place for any locally procured MoJ assets, and that an audit trail is available for inspection upon request by MoJ security.

Wherever possible and appropriate, managers should pool together equipment with that of local colleagues to share service costs.

If you have any concerns about moving items between sites securely, contact the Operational Security Team: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)

## Reusing equipment

When a project completes, or a colleague leaves or moves to a new role, equipment might become available. In many cases, it might be more cost-effective to consider reusing or reassigning this equipment, rather than disposing of it.

Any equipment must be completely 'cleaned' to an 'as-new' state before it is reused or reassigned. This means that all storage media in the device must be fully erased.

## NCSC Guidance

The NCSC provides useful guidance on secure disposal of electronic media, [here](https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media).

## Contacts

The following organisations are approved to help you with security disposal of equipment:

* TYR security: [g-cloud@tyr-security.co.uk](mailto:g-cloud@tyr-security.co.uk)
* Data eliminate: [info@dataeliminate.com](mailto:info@dataeliminate.com)

## Contact details

For any further questions relating to security, contact: [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

## Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [itpolicycontent@digital.justice.gov.uk](mailto:itpolicycontent@digital.justice.gov.uk).