#Equipment Reassignment Guide

##Introduction

This guide describes how to reassign equipment. It applies to laptops, mobile phones or other Ministry of Justice (MoJ) issued equipment. Reassignment is from one user to another.

##Who is this for?

This guidance applies to:

1. **Technical users**: these are in-house MoJ Digital and Technology staff. They are are responsible for implementing equipment controls. The controls apply throughout technical design, development, system integration, and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI, and Knowledge (EPICK) Team.
2. **Service Providers**: defined as any other MoJ business group, agency, contractor, IT supplier, or partner who in any way designs, develops, or supplies services (including processing, transmitting, and storing data) for, or on behalf of the MoJ.
3. **General users**: all other staff working for the MoJ.

“All MoJ users” means General users, Technical users, and Service Providers.

##Returning Equipment

When a project completes, or a colleague leaves or moves to a new role, equipment no longer required **SHALL** be returned. The Line Manager (LM) is responsible for using the Service Catalogue to request a return of the item. The equipment might then become available for use by other employees. It might not be cost-effective to consider reusing or reassigning the equipment. Possible reasons include:

* Older technology that might have been heavily used.
* The likelihood of operating problems and failures.
* Lack of support, updates, or patches.
* Slower performance.

As a result, it might be preferable to use a new machine, rather than repurposing a reassigned device. The decision depends on the expected use of the reassigned device.

The LM is responsible for ensuring a review of the equipment. This is to ensure that sensitive data **SHALL NOT** be lost by erasing the contents of the device. This task **CAN** be delegated to the team member most familiar with the data. The LM remains responsible. Any sensitive data identified **SHALL** be copied and relocated to a secure location. This can be the MoJ Teams facility or to Sharepoint. This **SHALL** happen before the device is made ready for reuse or destroyed.

Any IT equipment which is no longer needed, or has reached its “end of life” **SHALL** have its data securely deleted and confirmed to be unreadable and unrecoverable before destruction, redistribution, or reuse of the equipment.

##Equipment Reassignment

Equipment **CAN NOT** be passed from one user to another without being formally reassigned.

Equipment **SHALL** be completely “cleaned” to an “as-new” state before it is reused or reassigned. This means that all storage media in the device **SHALL** be fully erased. A sufficiently secure method for “wiping” equipment **SHALL** be used. Deleting visible files, emptying files from the “Recycle Bin” of a computer, or reformatting a device are not considered sufficiently secure methods for wiping equipment. The reason is that data recovery software might be used by a new owner to “undelete” files or “unformat” a device.

To erase data securely, use appropriate “data-shredding” tools for the media being erased. Typically, these tools do not simply delete data, they overwrite it multiple times. The overwriting erases all traces of the data, making it almost impossible for any retrieval. Another option is to re-encrypt the device using a different password, then delete the data to free up space.

Equipment reassignment **SHALL** be recorded by the LM in the appropriate asset register.

##Equipment that cannot be reused

If IT assets are no longer needed by the MoJ, and cannot be securely wiped, then the equipment **MIGHT** need to be destroyed physically. More information can be found at [Secure disposal of IT equipment](/guidance/security/it-computer-security/secure-disposal-of-it-equipment/)

Regrettably, for security reasons, redundant IT equipment **SHOULD NOT** be donated to charities, schools, or similar organisations.

##Leased equipment

Managers **SHOULD** ensure that any equipment that is leased has a data destruction clause written into the contract. Under such an arrangement, the supplier **SHALL** ensure that data is wiped when it is returned.

##Contacts

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

##Feedback

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