#Guidance on IT Accounts and Assets for Long Term Leave

##Audience and Document Purpose

This document is intended for Ministry of Justice (MoJ) line managers who have a staff member going on any type of long-term secondment, loan, or leave. It provides guidance on how to handle the IT accounts and IT assets (such as desktops, laptops, or mobile phones) of the staff member while they are on leave.

Long term means longer than 2 months.

Types of secondment, loan, or leave where this might apply include:

* Adoption Leave.
* Career Break.
* Loan.
* Maternity Leave.
* Secondment.
* Shared Parental Leave.

For the purpose of this guidance, all of these are examples of “long-term leave”.

##Guidance Statement

##Retaining assets, and access during leave

This guidance applies to assets, defined as being laptops, desktops, or mobile phones.

* A staff member going on any long-term leave may keep their assets while they remain contractually employed by the MoJ, **AND** where the leave is not longer than 12 months in duration.
* Remind your staff member that the Acceptable Usage Policy applies at all times during their leave. The policy can be found [here](/guidance/security/it-computer-security/acceptable-use/).
* Preparation or return from any type of leave may be accompanied by changes in working patterns. The Remote Working guidance provides useful advice for anyone who may be working remotely for the first time. The policy can be found [here](/guidance/security/emergencies/coronavirus-guidance/security/remote-working/).

**Note:** Devices that are not used for 3 months or more go in to a technical “quarantine”, intentionally to render them unusable. Staff members should log in to their devices once per month during leave, to ensure that technical quarantine is not activated. Logging in also helps ensure that system updates are downloaded and applied.

##Reviewing access to data and information systems

Before the staff member goes on leave, review their access to data and information systems, to ensure that this meets an ongoing need. This means that:

* If the staff member’s role is planned to change on their return to the MoJ, consider removing access now to data and information systems which they will no longer need. If their role is not planned to change on their return, you might consider leaving access “as-is” currently.
* Consider removing access to data or information systems which are OFFICIAL-SENSITIVE. This is in line with the necessity rigorously to apply the “need to know” principle for OFFICIAL-SENSITIVE information. See the guidance on classifying information for more detail </guidance/knowledge-information/protecting-information/classifying-information/>

##When to remove access and return assets

In a number of circumstances assets should be returned and access should be removed. This is where:

* The leave is longer in duration, and there is no business need or individual need for the user to keep assets and access. This should be considered for any leave above 12 months in duration. This is likely to be for Career Breaks or Loans.
* The staff member has no means of securely storing the asset, for example locking it securely in their home.
* Staff members going on leave for less than 12 months may return their assets and have access removed if they choose to do so.
* Line managers are empowered to determine whether the staff member should keep assets and access, as long as there is appropriate business justification, and staff members are appropriately supported. For example, a communication mechanism for keeping in touch is agreed.
* If, during their leave, the staff member decides to end their employment (resign), their line manager is responsible for following the appropriate leaver’s process with them. Refer to the Resignation section of the HR guidance and forms, with particular reference to the Leavers Checklist for Managers. This can be found at: </guidance/hr/end-change-of-employment/resignation/>

##How to remove access and return assets

* Access to systems and return of assets can be organised through the appropriate items in the [MoJ Technology Portal](https://mojprod.service-now.com/moj_sp). Please see the Knowledge Base article on “Returning your MoJ laptop, accessories and mobile phones” for details. Removal of access to local systems should be arranged with local IT teams.

**Note:** When a Dom1 account is deactivated, its data is recoverable for up to 12 months. See the Knowledge Base article on “How to Re-instate a Deactivated Email Account or Mailbox”.

##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).