Ofcom
making communications work
for everyone

Asset Management Policy

About this policy

This policy defines Ofcom's requirements around the recording of ICT assets, including the purchasing, supporting, and disposing of ICT assets. In addition, Assets are often issued to colleagues, 3rd parties and other contractors for them to fulfil their roles. These assets must be returned when the relationship ends between Ofcom and the person or entity to that the asset was issued.

Policy document

Version number: 2.5
Publication date: September 2019
Next revision date: June 2024

Owner's name: [redacted]
Owner's job title: Head of Service Delivery
Approved by: Security Committee

1 Purpose

1.1 This document sets out the policies that are required to ensure ICT assets are procured, supported and disposed of securely.

2 Scope

2.1 This policy covers all ICT assets like physical hardware and software but excludes information assets such as data or process documentation. Information assets are covered in the Information Security Policy.

3 Responsibility for ICT Assets

a) Inventory of ICT Assets

3.1 Identifying and documenting the importance of Ofcom's assets ensures Ofcom retains accurate records, has a realistic view of its ICT assets, and understands the potential impact on each ICT asset'. Anyone involved in purchasing software or managing or supporting hardware or software is responsible for the listed requirements below.

3.2 All ICT assets associated with information and information processing must be recorded and tracked in an asset register – these asset types include software assets, physical assets and services.

3.3 All Ofcom's ICT assets must be clearly identified and inventoried based on documented standards and procedures that cover the following:

- recording of hardware and software in an ICT asset register
- keeping the asset register up to date
- maintaining the accuracy of details in the register.

3.4 The ICT asset register may consist of multiple sources. Where possible, entries in the main register system must not be duplicated with other asset inventories but should be referenced to ensure that ICT asset entries are consistent.

3.5 Types of hardware to be recorded in an ICT asset register must include but are not limited to, computer equipment, mobile devices, network storage systems, network equipment, telephony equipment, conferencing equipment, portable storage media, authentication hardware, and any specialist equipment.

3.6 Types of software (including licensing details) to be recorded in an ICT asset register must include but not be limited to the operating system and virtualisation software, enterprise software, commercial-off-the-shelf software, and security software.

3.7 ICT asset registers must specify important information about each ICT asset, including but not limited to:

- the purpose of each ICT asset and corresponding owner.
- a description of hardware and software in use.
- versions of hardware and software in use (including patch levels);
- the location of hardware and software in use and details of portability (i.e., the extent to which the asset can change location);
- to whom the ICT asset is assigned.
- details of asset usage compliance requirements; see also the Acceptable Use Policy.
- licensing details (e.g., license keys and proof of ownership);
- key dates associated with support and maintenance.
- obsolescence details; and
- information necessary to recover from a disaster, including the type of asset, location, backup information, license information, and its Business Impact.

3.8 The ICT asset register must be protected against unauthorised change. Best efforts must be used to protect the inventory from errors. The asset register must be checked regularly to identify any discrepancies and ensure it is kept up to date.

3.9 The ICT asset register must consider externally hosted systems used to process Ofcom information e.g. outsourced services such as customer relationship management, email, room booking, expenses and People services.

3.10 All ICT assets must have a unique identifier.

3.11 ICT must ensure that the register of Ofcom ICT assets assigned to individuals is accurate.

b) Acceptable use of assets

3.12 The rules for the acceptable use of information and assets associated with information and information processing facilities are detailed in Ofcom's Acceptable Use Policy.

c) Return of Assets

3.13 All individuals must return all Ofcom's ICT assets in their possession upon termination of their employment, contract or agreement.

3.14 All Career and Performance managers must ensure that Leaver's forms are correctly completed for all Leavers they are responsible for. Career and Performance managers are also responsible for the collection of assets from Leavers.

3.15 The maintenance of the Joiners, Movers and leavers forms are jointly managed by ICT, People and Transformation and Internal Comms. The People and Transformation team are responsible for managing the Joiners, Movers, and Leaver's process.

3.16 Leavers must return ICT assets. Ofcom's policy is **not** to allow Leavers to keep assets they had previously used.

3.17 If a leaver fails to return an ICT asset, we reserve the right to require them to pay Ofcom an amount equivalent to the value of the ICT asset they have not returned. Failure to return ICT assets will also be considered theft and may lead to criminal prosecution by Ofcom.

4 Media Handling

4.1 Appropriate media handling ensures media is not lost, compromised, or tampered with. Physical (e.g., hard drives) and removable media (e.g., USB sticks) must only be used to transport information when the transfer cannot be achieved using a secure network connection, for example, when a secure network connection is unavailable for justifiable technical, financial, or operational reasons, or if the secured connection does not have suitable security controls to protect the sensitivity of the information.

a) Management of removable media

4.2 Information on removable media must be encrypted at rest. Information written to removable media must be encrypted unless an approved exception exists.

4.3 Removeable media must be stored in accordance with the manufacturers' recommended environmental tolerances.

4.4 Removeable media involved in critical processes must be tracked and have unique references. Removable media holding critical or sensitive information, including its current location must be maintained and should be included in the ICT Asset Register.

4.5 Removable media must be erased or destroyed appropriately. See the Disposal of Media below.

4.6 Removeable media should be appropriately labelled. Ideally, a low-profile label should be stuck on media that does not overtly identify Ofcom but has some identifying information on it so it can be returned to Ofcom if it is misplaced.

b) Disposal of media

4.7 Formal procedures for media disposal are necessary to ensure that media is disposed of securely and safely when no longer required.

4.8 Ofcom data held on media must be wiped before disposal or re-use.

4.9 An approved erasure mechanism must be used to wipe data. Media must be either physically destroyed or wiped using a multi-pass erasure application, which must, as a minimum, overwrite every sector of a filesystem multiple times. Flash or solid-state storage must be erased in line with the manufacturers' recommendations or physically destroyed. Solid state storage may not be properly erased using the techniques above due to the way data is stored.

4.10 Only approved companies may be used to dispose of media. All disposals must be undertaken by companies with which ICT have a standing relationship. ICT must ensure that the disposal company adheres to this policy.

4.11 An audit trail of disposed media must be held. Disposal companies must provide records of what media has been disposed of and, in the case of electronic media, provide certificates for each item containing a sample of the filesystem's data to demonstrate that the data has been overwritten.

4.12 Large quantities of non-sensitive data could become sensitive by the aggregation effect. Therefore, media accumulated for disposal should be held securely to guard against this risk.

c) Physical media transfer

4.13 Technical and procedural controls are required to protect media containing Ofcom information against unauthorised access, misuse, or corruption during transportation.

4.14 Standards for protecting physical media in transit must be developed and communicated to all applicable users.

4.15 Removable media must always be encrypted. If it is not possible to encrypt media (e.g., hard drives) that contains sensitive information, additional physical protection of the media should be considered.

2. Additional information

Version History

Version number	Version date	Revised by	Description of changes made
V2.0	15/11/2017	[redacted]	Creation of document
V2.1Draft	15/02/2018	[redacted]	Updated as part of ISO27001 review. Removed references to Information Security – this is covered by Information Security Policy.
V2.1	22/02/2018	[redacted]	Updated changes to remove inconsistent use of the terms, media, removable media and ICT Assets.

Version number	Version date	Revised by	Description of changes made
			Amended non-return of ICT assets to reflect possible criminal consequences.
V2.2	27/09/2019	[redacted]	Reviewed by Security Committee
V2.3	21/09/2020	[redacted]	Reviewed internally by ICT
V2.4	05/06/2022	[redacted]	Reviewed internally by Service Management
V2.5	24/04/2023	[redacted]	Replaced line manager with Career and Performance manage, and clarified 3.17 where it says "may" to **must** return ICT assets and changed where it mentions compliance policy to Acceptable Use Policy

Distribution

Name	Action required	Date required by
Security Committee	SC 26 (19)	28/05/2019