

Media Handling Rules for JTrack

1. Definition

The term “media” covers all means by which information can be imported to the system or exported from it. This includes but is not limited to:

- a) Paper Hardcopy
- b) Magnetic media; floppy discs, tape, hard disk drives etc.
- c) Optical media such as CDs and DVDs in all formats etc.
- d) USB memory devices; memory sticks, mini disk drives etc

2. Scope

- a) The following rules shall be followed by **all** non privileged users of the system regardless of their parent organisation. Privileged users such as Cable & Wireless system and application administrators should continue to use their existing procedures.
- b). The following rules have had to make the assumption that **non privileged users may create media for export/import**, until the business process is better understood. It is recommended that this process be limited to staff with import/export authority in user organisations.

3. Interim Media Handling Rules

1. Hardcopy output shall be marked at the top and bottom of each page with the protective marking of the information and the resulting document handled in accordance with that marking. Individual softcopy files of information should also contain the protective marking in the body of the information (if it is a document) or in the file title if this is not possible.
2. Use fresh media for each information export from the system¹.
3. Users shall be responsible for ensuring that media created from information exported from the system shall be physically marked with the **maximum** protective marking of the information it contains (assuming more than one file is exported) and the media thereafter handled in accordance with that marking. USB sticks and other small format media shall have a separate label attached with the marking clearly shown on the label.

NOTE: It is recommended that fresh physically marked media be dedicated to NOT PROTECTIVELY MARKED, PROTECT, RESTRICTED and (if needed) CONFIDENTIAL material, and that **no material exceeding these markings** should be written to such media.

4. Media containing information protectively marked above RESTRICTED shall not be used to import information onto the system.
5. Media export from the system shall only be undertaken when necessary to perform a user’s task. The **minimum** information required to support a business process/exchange should be exported to the media. Please note that where the complete system database is copied to media the media shall thereafter be marked and handled as CONFIDENTIAL.

¹ This avoids the complex procedures required for secure overwriting/erasure in order to re-use media at a different protective marking to the original.

6. Where media are to be transported to another physical site or otherwise outside the secure premises of the organisation that created the media the transport rules in Appendix A should be followed. Under **no** circumstances should media be left insecure.
7. Each organisation that exports information to the system on media, or imports information contained on such media to the system, shall set up and maintain an import/export **media register** that records, as a minimum, the following information:
 - a) Originator name and organisation/tally
 - b) Media number or other unique identifier
 - c) Brief meaningful description of content
 - d) Protective marking (NOT PROTECTIVELY MARKED, PROTECT, RESTRICTED with any descriptors)
 - e) Destination address, including nominated recipient name/tally
 - f) Date and time of media creation or
 - g) Date and time of recipients media receipt
8. Record Import/Export media destruction in the media register.
9. Media **must** be destroyed in a secure manner according to protective marking when no longer required:
 - a) paper marked at or above RESTRICTED must be cross-cut shredded before disposal using a Government approved method.
 - b) other media must be securely destroyed according to the protective marking using Government approved methods.

Appendix A Media Transport Rules

Protective Marking/ Transport Requirements	PROTECT	RESTRICTED	CONFIDENTIAL
1. Movement within single organisation via Internal Despatch	<p>By trusted hand OR In a sealed envelope or container with protective marking and descriptor clearly shown</p> <p>Data on Magnetic or optical media must be encrypted using an approved product to at least FIPS 140-2 standard before media despatch</p>	<p>By Trusted Hand OR</p> <p>In a sealed envelope or container with protective marking and descriptor clearly shown.</p> <p>Transit envelopes may be used if sealed with the appropriate security label.</p> <p>Data on Magnetic or optical media must be encrypted using an approved product to at least FIPS 140-2 standard before media despatch</p>	<p>By Trusted Hand OR</p> <p>In a secured container or using double envelopes both fully addressed, but with the protective marking and descriptor shown on the inner envelope only.</p> <p>Show a return address on the outer envelope.</p> <p>Data on Magnetic or optical media must be encrypted using a CESP approved product to protect CONFIDENTIAL data as a minimum.</p>
2. Movement within UK	<p>By Trusted Hand in a closed envelope or container OR</p> <p>By post or courier service, in a sealed envelope with no protective marking or descriptor shown and addressed to an individual by name or appointment.</p> <p>Data on Magnetic or optical media</p>	<p>By Trusted Hand in a closed envelope or container OR</p> <p>By post or courier service, in a sealed envelope with no protective marking or descriptor shown and addressed to an individual by name or appointment</p> <p>Data on Magnetic or optical media must be</p>	<p>Carried only by Trusted Hand, or post or courier in a secured container or using double envelopes, both fully addressed, but with the protective marking and descriptor shown on inner envelope only</p> <p>Show a return address on outer envelope.</p> <p>Document transmission and receipt must be recorded in a secure register in sending and receiving organisations.</p> <p>Data on Magnetic or</p>

	must be encrypted using an approved product to at least FIPS 140-2 standard before media despatch.	encrypted using an approved product to at least FIPS 140-2 standard before media despatch.	optical media must be encrypted using a CESSG approved product to protect CONFIDENTIAL data as a minimum.
--	---	--	--