INFORMATION HANDLING QUICK REFERENCE GUIDE

	MARKING			ACCESS				MOVING INFORMATION / ASSETS				DISPOSAL	LOSS
Hard Copy information and Digital information on electronic media such as CD, DVD and memory sticks	Classification Marking required	Classification marking can only be changed with originator's permission.	Should consider including handling instructions	For RoS internal use only, unless management has approved external dissemination	Made available strictly on a "need to know basis"	Is likely to be disclosable under a request for access under "Freedom of Information legislation"	Must be locked securely away when not in use or unattended.	Can be left in RoS correspondence tray / mail room pigeon hole.	Can be sent using standard reputable post / courier service.	Bulk transfers (over 1000 records) permitted.	Must obtain authority of Senior Management before taking information out of RoS premises.	Dispose of with care using approved commercial disposal products to make reconstitution unlikely.	Must report immediately compromises / losses to line management.
Routine OFFICIAL	✗	N/A	✗	✓	✗	✓	✗6	✓	✓8	✓10	✓11	✓12	✓
OFFICIAL with a sensitive nature but doesn't meet **OFFICIAL-SENSITIVE** criteria	✗	N/A	✓4	✓	✓	✓5	✓	✗7	✓9	✓10	✓11	✓13	✓14
OFFICIAL-SENSITIVE	✓1	✓3	✓4	✓	✓	✓5	✓	✗7	✓10	✓10	✓11	✓13	✓14
Protectively marked non HMG material	✗2	✓3	✓4	✓	✓	✓5	✓	✗7	✓9	✓10	✓11	✓13	✓14
Information entrusted to RoS relating to our registers[1]	✗	N/A	✗	✓	✗	✓5	✗6	✓	✓	✓10	✓11	N/A	✓
Other third party material with no classification marking	✗	N/A	✗	✓	✗	✓5	✗6	✓	✓	✓10	✓11	✓12	✓

NOTES:

1. The use of this handling caveat will be rare in RoS & should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' as compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation or for HMG more generally. The requirement to use the OFFICIAL-SENSITIVE marking should also be agreed with the IAO.
2. If a third party's information is considered OFFICIAL-SENSITIVE, which should be a rare event, then the container that holds this information should have an OFFICIAL-SENSITIVE marking.
3. Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument.
4. If the recipients will not be aware of RoS policy and guidance in respect to the handling, sharing and disposal of information then handling instructions should be completed and provided.
5. Every effort should be made to consult the originator or originating organisation, particularly so if a sensitive asset is requested for disclosure.
6. Staff must take due care of this information to protect it from loss and follow the RoS Clear Desk and Screen Policy. Personal data should be protected from unauthorised access at all times.
7. Must be hand delivered to the person. If person not available should not be left unsecured. The information should be placed inside RoS secure container bags when transmitted between RoS premises.
8. Include return address. Single closed cover / envelope.
9. Include return address. Consider using registered Royal Mail service or reputable commercial courier's track and trace service. Single closed cover / envelope. In addition, if the material is held on electronic media then encryption should be used.

[1] RoS in its statutory capacity receives and temporarily holds information which is not protectively marked (for example documentation supporting applications for registration, deeds for recording etc.), which is returned to the sender.

INFORMATION HANDLING QUICK REFERENCE GUIDE

10. Senior Management approval must be sought in the first instance. Include return address. Use registered Royal Mail service or reputable commercial courier's track and trace service. Consider double envelope. Where double envelopes are used the outer envelope must not have the classification marking applied, the inner cover should detail the classification marking. In addition, if the material is held on electronic media then encryption must be used where feasible. The transfer should also be recorded in an in house log.
11. Information taken outside the office in person by RoS staff should be carried in an appropriate container & not left unattended in a public place. Sensitive material on electronic media must be encrypted where feasible.
12. The RoS bins assigned for paper disposal are adequate as the paper is securely destroyed using a third party service. Electronic media should be handed to the IT Service Desk for secure disposal. Destruction of information constituting corporate records must always be recorded and notified to the Records Manager.
13. It is recommended that the destruction should be witnessed by the person disposing of the information so a RoS shredder should be used rather than using a third party service. Electronic media should be handed to the IT Service Desk for secure disposal. Destruction of information constituting corporate records must always be recorded and notified to the Records Manager.
14. The Departmental Security Officer, Information Asset Owner and SIA team must be advised. Where there is significant compromise / loss of personal information the Information Commissioners Office must be advised.

	MARKING			**ACCESS**			**TRANSMISSION**			**LOSS**
E-mail and Instant Messaging Note Instant Messaging is not used widely in RoS. External Instant messaging should never be used to transmit information of a sensitive nature.	Classification marking required	Classification marking can only be changed by the originator's permission.	Should consider including handling instructions.	For RoS internal use only, unless management has approved external dissemination	Made available strictly on a "need to know basis"	Is likely to be disclosable under a request for access under "Freedom of Information legislation"	Can be sent internally over the RoS email system to RoS email addresses	Can be sent to non RoS email addresses.	Email of bulk data (over 1000 records) permitted	Must report instances to management where emails sent to wrong recipient(s)
Routine OFFICIAL	✗	**N/A**	✗	✓	✗	✓	✓	✓ **6**	✓ **8**	✗ 9
OFFICIAL with a sensitive nature but doesn't meet OFFICIAL-SENSITIVE criteria	✗	**N/A**	✓ **4**	✓	✓	✓ **5**	✓	✓ **7**	✓ **8**	✓ 9
OFFICIAL-SENSITIVE	✓ **1**	✓ **3**	✓ **4**	✓	✓	✓ **5**	✓	✓ **8**	✓ **8**	✓ 9
Protectively marked non HMG material	✗ **2**	✓ **3**	✓ **4**	✓	✓	✓ **5**	✓	✓ **7**	✓ **8**	✓ 9
Information entrusted to RoS relating to our registers	✗	**N/A**	✗	✓	✗	✓ **5**	✓	✓	✓ **8**	✗ 9
Other third party material with no classification marking	✗	**N/A**	✗	✓	✗	✓ **5**	✓	✓	✓ **8**	✗ 9

NOTES:

1. The use of this handling caveat will be rare in RoS and should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' as compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation or for HMG more generally. The requirement to use the OFFICIAL-SENSITIVE marking should also be agreed with the IAO.
2. If a third party's information is considered OFFICIAL-SENSITIVE, which should be a rare event, then any replies should have an OFFICIAL-SENSITIVE marking.
3. Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument.
4. If the recipients will not be aware of RoS policy and guidance in respect to the handling, sharing and disposal of information then handling instructions should be completed and provided.

INFORMATION HANDLING QUICK REFERENCE GUIDE

5. Every effort should be made to consult the originator or originating organisation, particularly so if a sensitive asset is requested for disclosure.
6. E-mails may quickly become sensitive, as material is added or as new recipients are copied in. The recipient should assess the entire contents of an e-mail thread before they add to it and forward it on to ascertain if the email's sensitivity has risen.
   Note RoS material must not be emailed by an individual to their personal webmail address to work on out of office unless permission has been given by the IAO.
7. Consider using a secure mechanism (such as email encryption). Where a recipient has a PSN or GSI email address, consider emailing over the Government secure private network, the SIA team can offer advice on these. Note sensitive material must not be emailed by an individual to their personal webmail address to work on while out of office.
8. A secure mechanism such as email encryption must be used. Where a recipient has a PSN or GSI email address, consider emailing over the Government secure private network, the SIA team can offer advice in these. Note sensitive material must not be emailed by an individual to their personal webmail address to work on out of office.
9. Any instance of loss or compromise of personal data relating to individuals must be immediately notified to the Data Protection Officer

	DISCUSSION	**FAX**	**ANSWER MACHINES**
Voice and telephony	Must not be discussed in a public area where unauthorised personnel could overhear the conversation.	Sender to phone recipient to advise fax is being sent and confirm a trusted person is waiting at the fax machine that the document is being sent to.	Details of sensitive material should be kept to a minimum when leaving messages on answer phone or voice mail systems as recipient may not have setup their system securely and messages could be accessed by others.
Routine OFFICIAL	✗	✗	**N/A**
OFFICIAL with a sensitive nature but doesn't meet OFFICIAL-SENSITIVE criteria	✓	✓	✓
OFFICIAL-SENSITIVE	✓	✓	✓
Protectively marked non HMG material	✓	✓	✓
Information entrusted to RoS relating to our statutory registers	✗	✗	**N/A**
Other third party material with no classification marking	✗	✗	**N/A**

INFORMATION HANDLING QUICK REFERENCE GUIDE

	PROTECTION AT REST				CARRIAGE			DISPOSAL	LOSS
IT equipment / components	Operational equipment must be password locked when unattended.	Data on equipment must be protected with approved HMG encryption.	Equipment must be located in a secure area, with access controlled by a physical access control system.	Equipment must be physically secured by a key operated security cable to help prevent / deter theft.	Can be transported within a RoS building without any special protective measures being applied.	Can be transported between RoS buildings without any protective measures being applied other than taking an inventory audit before delivery commences, then another inventory audit at the delivery destination.	Can be transported to non RoS buildings without any protective measures being applied other than taking an inventory audit before delivery commences, then another inventory audit at the delivery destination.	Must be disposed of in a secure manner to make re-constitution of data unlikely.	Must report immediately compromises / loss to line management.
Server equipment	✓	✗	✓	✗	✓ 2	✓ 3	✓ 4	✓ 5	✓ 6
Server components (such as hard disks)	**N/A**	✗	✓	✗	✓ 2	✓ 3	✓ 4	✓ 5	✓ 6
Desktop equipment (such as PCs and DMS workstations)	✓	✗	✗	✗	✓ 2	✓	✓ 4	✓ 5	✓ 6
Portable equipment (such as laptops, tablets)	✓	✓	✗	✓ 1	✓	✓	✓	✓ 5	✓ 6

NOTES:

1. All RoS laptops must be physically protected by a cable lock when left unattended. Cable lock protection for tablets is not required but tablets must never be left unattended unless locked away.
2. Must be conducted under the supervision of the IT Service.
3. Must use a reputable fully insured courier / removal service if not conducting the move using RoS transport and personnel.
4. Must obtain the consent of the appropriate IAO before removing equipment from RoS premises that contains data that the IAO is responsible for.
5. IT support arrangements with 3rd parties provide services where faulty IT equipment parts are replaced with new parts, with the original faulty parts then transferring ownership to the 3rd party. It is important in these instances where parts are replaced, such as hard disks, to have arrangements in place with the 3rd parties to ensure that any data residing on the replaced parts will be deleted securely. The SIA team also require a disposal certificate or copy of to ensure destruction in line with HMG policies.
6. The Departmental Security Officer, Information Asset Owner and SIA team must be advised. Any instance of loss or compromise of personal data relating to individuals must be immediately notified to the Data Protection Officer.