Handling information based on the protective marking

	OFFICIAL	**OFFICIAL-SENSITIVE** **In Addition to OFFICIAL**
INFORMATION MARKING		
Legal and statutory obligations, in particular under the Data Protection Act, will be followed, whatever the protective marking used.		
General points	• Be stored and managed securely within MRC approved systems • Handled in line with local guidance on open-plan working and clear desk principles. • Not be accessed, read or discussed where you can be overlooked or overheard	• Not be left unattended and should be locked away when not in use. • Only communicated or passed to others on a need to know basis
Emailing material	▪ By default this information can be sent in the clear over the Internet. ▪ No restrictions on emailing information, however it should be limited on a 'need to know' basis. ▪ You may choose to include additional handling tag and/or instructions, if appropriate. ▪ When receiving email you must follow any handling guidance stipulated by the sender. ▪ Where necessary adopt the transmission technique as used by the sender (eg, encryption of message if sending outside your email domain). ▪ Where information you have added has increased the sensitivity you may choose to password protect or encrypt to provide additional protection.	▪ Permitted to known contacts on a 'need to know' basis. ▪ You must follow the document originator's lead on encryption when replying to or forwarding emails. ▪ Information should normally be sent by encrypted e-mail. ▪ Information can be sent unencrypted only after making a risk based decision on the likelihood of it being intercepted and the level of damage that may be caused. ▪ Consider using password protection where encryption is not appropriate.
Moving information - by hand or post	**BY HAND:** ▪ Protect at least by one cover/envelope. ▪ Authorisation should be obtained from the	▪ Carry in a nondescript bag in order to not draw attention to the contents.

	OFFICIAL	OFFICIAL-SENSITIVE In Addition to OFFICIAL
	Information Asset Owner if moving a significant volume of assets / records / files. **BY POST/COURIER:** ▪ Use single, unused envelope. **MOVING ASSETS OVERSEAS (BY HAND / POST / COURIER):** ▪ Use single, unused envelope.	▪ Never leave papers unattended. ▪ Include return address on back of the envelope. ▪ Never mark the classification on envelope. ▪ Consider double envelope for highly sensitive assets (write the classification on the inner envelope only). ▪ Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service. Either by: ▪ Trusted hand under single cover; *or:* ▪ Include return address on back of the envelope. ▪ Never mark the classification on envelope. ▪ Consider double envelope for highly sensitive assets (and writing the classification on the inner envelope only). Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service.

	OFFICIAL	**OFFICIAL-SENSITIVE** **In Addition to OFFICIAL**
Faxing	Faxes should not be assumed to be secure. Consider using encrypted email if possible to communicate sensitive information.	
	▪ Confirm the recipient's fax number. ▪ Recipients should be waiting to receive faxes containing personal data marked OFFICIAL.	▪ Sensitive material to be faxed should be kept to an absolute minimum.
Printing	▪ Permitted – but print only what you need and consider PIN printing. ▪ All printed materials must be disposed of appropriately when no longer required or being used.	
Photocopying	▪ Permitted – but make only as many copies as you need, and control their circulation. ▪ Consider PIN printing/copying where appropriate.	
STORAGE		
Physical storage (of documents, digital media, when not in use)	▪ Protect in line with local guidance on open-plan working and clear desk principles. This may include: protecting physically within a secure building by a single lock (eg a locked filing cabinet, locked drawer or container); not leaving papers on desks or on top of cabinets overnight. Laptops must be locked away or secured in docking stations when left in the office, only encrypted laptops may be taken outside of an MRC establishment.	
Electronic storage	▪ Any electronic document received marked OFFICIAL should be saved with OFFICIAL in the title and also in electronic document and records management system metadata or notes fields. ▪ Appropriate controls should be used to limit access.	▪ Any electronic document received marked OFFICIAL-SENSITIVE should be saved with OFFICIAL-SENSITIVE in the title and also in electronic document and records management system metadata or notes fields. ▪ Appropriate controls must be used to limit visibility of the document and access.

	OFFICIAL	**OFFICIAL-SENSITIVE** **In Addition to OFFICIAL**
Electronic storage on digital media (USB memory sticks, CDs, DVDs)	▪ Only MRC supplied and approved portable media is to be used. ▪ The media must be encrypted. ▪ Delete protectively marked information held on digital media only within MRC buildings and on MRC computer systems.	
Disposing of documents	Dispose of documents appropriately. ▪ Information already in the public domain can be disposed of by recycling or as ordinary waste. ▪ Information marked OFFICIAL or OFFICIAL-SENSITIVE must be disposed of with care, either using a secure disposal bin or by shredding using an approved cross-cut shredder.	
REMOTE WORKING		
General points	▪ Laptops and removable media used to store OFFICIAL and OFFICIAL–SENSITIVE information must be encrypted. ▪ Information marked OFFICIAL or OFFICIAL-SENSITIVE must not be emailed to or from home/personal e-mail accounts. ▪ Limit the amount of information you take out of the office. Only take what is necessary. Refer to local guidance on remote working and 'Bring your own device' and contact your local IT Manager or the IT Security team at head office for further information.	
Telephone, videoconferencing and other tools	**You should not assume telephony systems, video conferencing or tools such as Microsoft Lync and Skype are secure.**	
	▪ No restrictions but be careful of how your	▪ Details of OFFICIAL-SENSITIVE material should be

	OFFICIAL	**OFFICIAL-SENSITIVE** **In Addition to OFFICIAL**
	discussion might be perceived by others in earshot and of straying into areas that could be deemed as OFFICIAL–SENSITIVE.	kept to an absolute minimum and should only be discussed where there is no risk of being overheard.