Appendix 2

GOVERNMENT SECURITY CLASSIFICATION SCHEME

1. The vast majority of information held by the Office of the Police and Crime Commissioner (OPCC) will be at the level of OFFICIAL.

2. The table below describes standard control measures when working with information assets at **OFFICIAL** (including **OFFICIAL – SENSITIVE**).

	OFFICIAL including OFFICIAL-SENSTIVE
Personnel Security	▪ All staff, volunteers, contractors etc. must have appropriate vetting clearance

Physical Security
 	
a. Document handling
	▪ No requirement to mark documents with **OFFICIAL** marking
	▪ Comply with the Clear Desk Policy
	▪ **OFFICIAL-SENSITIVE** the document must be marked at the top and bottom of each page and handling instructions considered, e.g.
	  ▪ FOR OPCC EYES ONLY
	  ▪ TO BE OPENED BY ADDRESSEE ONLY
	  ▪ NOT FOR FORWARD DISSEMINATION
	  ▪ NO PHOTOCOPYING WITHOUT PERMISSION OF ***AUTHOR***

b. Storage	▪ Storage behind a single locked barrier. **OFFICIAL – SENSTIVE** – consider a second locked barrier. ▪ **OFFICIAL-SENSITIVE** - Consider use of approved physical security equipment/furniture
c. Remote Working	▪ Ensure information cannot be inadvertently overlooked whilst being accessed remotely ▪ Store assets under lock and key at remote locations
d. Moving assets by hand	▪ Single cover with no external markings – sealed transit envelope is acceptable ▪ **OFFICIAL-SENSITIVE** – Sealed envelope – no external markings ▪ Precautions against overlooking when working in transit (e.g. whilst travelling by train)
e. Moving assets by post/courier	▪ Sealed envelope, never mark classification on envelope ▪ **OFFICIAL-SENSITIVE** - Consider double enveloping ▪ If sending sensitive personal data externally use registered Royal Mail service or reputable commercial courier's 'track and trace' service
f. Moving assets overseas	▪ Sealed envelope, include return address, never mark classification on envelope ▪ Trusted hand under single cover (Contact Information Security Officer in PSD for advice)
g. Bulk Transfers	▪ Authorisation from Information Asset Owner required for significant volume of records/files

	OFFICIAL including OFFICIAL-SENSTIVE
	▪ Contact Force Information Security Officer for advice and risk assessment
INFORMATION SECURITY a. Electronic Information at Rest	▪ Electronic data at rest can be found on computers, mobile devices etc. This information is protected according to its sensitivity; for portable devices data will be encrypted. ▪ Appropriate controls to protect the information may be physical protection, such as a locked door or may involve encrypting data that would be classified as **OFFICIAL-SENSITIVE**
b. Electronic Information in Transit e.g. e-mail	▪ Remember, ALL emails are at least **OFFICIAL** ▪ Information between OPCCs, Police forces, government and trusted organisations is via secure networks, e.g. '.pnn' e-mail ▪ If the email does not contain sensitive information you can send it over the insecure internet e.g. anyone@anywhere.com ▪ Do not send sensitive information to insecure internet domain addresses, such as Google mail, Hotmail, Yahoo, consider redacting the information if appropriate ▪ Where more sensitive information must be shared with external partners or members of the public, consider using secure mechanisms such as password protected documents. Consider file encryption for **OFFICIAL-SENSITIVE** together with handling instructions. ▪ Where more sensitive information must be shared with external partners, ensure secure mechanisms (e.g. browser sessions using SSL/TLS) are used. Consult the Information Security Officer in PSD for advice ▪ You should provide handling instructions if necessary, based on your risk assessment and at **OFFICIAL-SENSITIVE** ▪ In **exceptional** circumstances, where there is a requirement for information to be sent unencrypted over the Internet, you have to make a risk-balanced decision; there is always a risk of information being intercepted and exposed. It is very important to stipulate handling instructions in this scenario. ▪ You must follow any handling guidance stipulated by the relevant Information Asset Owner
c. Removable Media (data bearing)	▪ All portable and removable media must be encrypted and only Force supplied devices are to be used ▪ Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement
d. Telephony (mobile and landline), Radio, Video Conference and Fax	▪ Details of sensitive material should be kept to a minimum – be aware of being overheard and your surroundings ▪ Your conversation, video conference etc. may be recorded by the other or a third party ▪ Faxing is only acceptable as a last resort, where the recipient does not have a secure e-mail and there isn't time to send via post ▪ Recipients should be waiting to receive faxes containing personal data and/or data marked with the **OFFICIAL – SENSITIVE** caveat
Disclosure	▪ Where appropriate, non-sensitive information should be published by the OPCC for reuse. ▪ Statutory disclosures are separate from the classification scheme and require case-by-case assessment ▪ Requests for release under the Freedom of Information Act should be referred to the OPCC Corporate Administration Officer

	OFFICIAL including OFFICIAL-SENSTIVE
	▪ The release of personal data is subject to the Data Protection Act principles. Contact the OPCC Corporate Administration officer for advice.
Destruction of Hard Drives etc.	▪ All disposal of IT equipment must be carried out by the Force IT Department
Disposal / Destruction of paper	▪ Destroy using equipment which meets a recognised international paper destruction standard, designed to consistently destroy to particles no larger than 4 x 15 mm
Incident Reporting	▪ Inform your line manager and complete the relevant Force Incident reporting form ▪ Follow incident reporting procedures set out in the relevant Force Security Policy