Guidance 1.1: Working at OFFICIAL

What is OFFICIAL classified information?

1. All information that is created or processed by organisations subject to the GSCP is OFFICIAL by default, unless it is classified at a higher level. The majority of government information is classified at OFFICIAL and many users will work only at the OFFICIAL tier.

2. The OFFICIAL tier contains a huge volume of information at many different levels of sensitivity, ranging from information that is already in the public domain to information which may be of interest to highly capable threat actors, and whose compromise could cause harm (albeit not significant or long-term harm) to the UK, its people or its interests.

3. The information creator is responsible for assessing the expected threat profile to an information asset and the potential impact of an accidental (such as a data loss or incorrect disclosure) or a deliberate compromise, to determine the right classification, markings and controls to apply.

Application of the OFFICIAL classification tier

4. The need-to-know principle underpins decision making on OFFICIAL information. The information creator is responsible for determining whether a recipient needs-to-know; access to OFFICIAL information should always be no wider than is deemed necessary for business needs and be risk-based. The information creator must be assured that the recipient understands and possesses the relevant security controls necessary to protect the information.

5. The need-to-know must be balanced with the need-to-share: information is only valuable if it is used by those who need it. The balance between these two principles must be considered carefully. Typically, need-to-know controls will increase as the sensitivity of information increases, so as to reduce the risk of compromise.

6. Within the OFFICIAL tier, information or material whose compromise is likely to cause damage to the work or reputation of the organisation and/or HMG must be marked with the -SENSITIVE marking. OFFICIAL information that uses the -SENSITIVE marking may be subject to additional controls to protect need-to-know.

7. The difference between OFFICIAL and OFFICIAL information marked -SENSITIVE is;

    a. OFFICIAL: Information whose compromise would typically cause limited to no negative consequences for HMG, our partners (including damage to confidence in the confidentiality between HMG and its partners) or to an individual. This includes information that has been cleared for publication (which should be denoted by the FOR PUBLIC RELEASE handling instruction). It also includes routine operational, policy and service information that is not intended for public release, but that is unlikely to be of interest to threat actors. Aggregated data sets of OFFICIAL information may warrant additional controls (see Guidance 1.5 - Considerations for Security Advisors)

    b. OFFICIAL information marked -SENSITIVE: Information that is not intended for public release and that is of at least some interest to threat actors (internal or external), activists or the media. OFFICIAL information that uses the -SENSITIVE marking is likely to be of interest to threat actors due to its sensitivity or topical significance. A compromise could cause moderate, short-term damage to: HMG, the UK's international reputation, the UK economy, HMG's relations with its partners (including international partners) or moderate harm or distress to an individual or group of people. The implications of a compromise could be potentially significant, but are not long standing and are unlikely to cause serious harm to HMG or the UK. Such information should be identified using the -SENSITIVE marking and additional handling controls apply.

8. OFFICIAL and OFFICIAL information marked -SENSITIVE each have a set of baseline behaviours which provide a level of protection that is proportionate to the level of risk. Organisations may need to apply security controls above the baseline on a risk-managed basis, which are appropriate to local circumstances and in line with organisational risk tolerances.

9. A wide range of personal information (including large identifiable data sets) can be handled at OFFICIAL. In all instances, organisations must fulfil their UK GDPR and DPA 2018 legal obligations. In determining whether a -SENSITIVE marking and the related additional controls should be applied, organisations should consider whether alternative risk management measures are proportional to the potential impact of the personal information being compromised. Particular consideration should be given to Special

Category Data, Criminal Offence Data and Childrens' Data, as defined by UK GDPR, and large aggregated data sets (see Guidance 1.5 - Considerations for Security Advisors).[1]

10. Clear direction and guidance must be set by an organisation's SA/SSA or Head of Security on working with personal information to ensure consistent and effective working practices. The organisation's Data Protection Officer (or equivalent) should be consulted when setting this direction and guidance.

11. Where OFFICIAL information has been cleared for publication or is already in the public domain, the information creator should where possible apply the FOR PUBLIC RELEASE handling instruction (in the format 'OFFICIAL-FOR PUBLIC RELEASE') to indicate that the information holds no sensitivity and can be shared without any restrictions, including with the general public. Use of this handling instruction is recommended, but is at the organisation's discretion; users should consult their local organisation's policy.

Application of the OFFICIAL baseline behaviours

12. When creating an information asset, such as a document or email, the information creator should apply the appropriate classification marking and decide whether any additional markings or handling instructions are needed, taking into account: any source material being used (e.g. other classified information assets); the sensitivity of the material; and, the people who need-to-know. OFFICIAL and OFFICIAL information marked -SENSITIVE should be handled in line with the recommended behaviours (associated with verbal, hard copy and electronic information) outlined in the table below, which are based on expected risks to and the impact of compromise to information of that sensitivity.

13. The behaviours must be reinforced by training to ensure that individuals understand their personal responsibilities within the classification and marking process. Line managers should role model and promote good security behaviours, and are responsible for ensuring their staff apply security classifications and handling instructions correctly. Organisations must use local policies to set out their expectations in more detail, to create and maintain a security culture commensurate with their particular risk and operating environment.

[1]Information Commissioner's Office. 'Special Category Data' (viewed on 16 June 2023); Information Commissioner's Office. 'Criminal Offence Data' (viewed on 16 June 2023); Information Comissioner's Office. 'Children's information' (viewed on 16 June 2023).

14. The baseline behaviours in the table below provide the basis for the development of local security controls; organisations can develop controls above the baseline to manage specific risks. If additional security controls and/or behaviours are necessary at a local level, the information creator should consult with their Security Adviser (or equivalent) to ensure the controls and/or behaviours are aligned with organisational policy and proportionate to the local risk appetite.

15. In general, it is expected that government systems will be used for government business. The processing of significant OFFICIAL information (and OFFICIAL information marked -SENSITIVE) on a privately managed device via non-corporate communication channels can only be justified in exceptional circumstances.

16. The use of non-corporate communication channels to process OFFICIAL sinformation, on government systems or private devices, requires users to exercise their professional judgement, assessing threats and other risks to the information. Further guidance is available on GOV.UK - see *Using non-corporate communication channels (e.g. WhatsApp, private email, SMS) for government business*.

OFFICIAL (Tier 1)		OFFICIAL information (Tier 1) marked -SENSITIVE
Intended use: • The OFFICIAL marking is for the justified distribution of information, which has either been cleared for publication or is not in the public domain but is of limited sensitivity, whose compromise would cause limited to no negative consequences to HMG. • The information can be shared across the organisation and partners based on need-to-share, without authorisation from the information creator, to support the efficient conduct of the organisation's business.		• The -SENSITIVE marking is for the limited distribution of more sensitive OFFICIAL information on a need-to-know basis. The information user should seek, where possible, authorisation from the information creator to share an asset outside of their organisation or to substantially expand the distribution list/circle of knowledge. The need-to-share information within the organisation without authorisation is justified to support the business of HMG.[2]
Baseline behaviours and measures:		
Verbal information	**Meetings & Discussions:** • Only discuss using corporate devices or devices that have been approved by your organisation:	**Meetings & Discussions:** • Only discuss on corporate devices or devices that have been approved by your organisation: ○ In public: do not discuss if you can be overheard

[2] The release of OFFICIAL information marked -SENSITIVE by contractors to parts of their organisation based overseas shall be in accordance with any approvals process mandated by the HMG Contracting Authority.

	○ In public: OFFICIAL information can be discussed freely, but be aware of whether you can be overheard by any unauthorised individuals, such as members of the public, or by smart listening devices. Information marked -FOR PUBLIC RELEASE can be discussed freely. ○ In the office: can discuss in publicly accessible parts of the building. ○ If working remotely: can discuss in shared spaces, but be aware of whether you can be overheard by smart listening devices. ● Always exercise particular care when discussing names and contact details and ensure that you are compliant with your organisation's policies and with data protection legislation. ● Meeting attendees can brief back to their teams as they see fit.	○ In the office: do not discuss in publicly-accessible parts of the building if you can be overheard. ○ If working remotely: only discuss in a private space. ● Meeting attendees can brief back to their team members within their organisation based on need-to-know, but should check with the information creator if sharing further.

Hard copy information	**Storage & Access** ● Only print on corporate systems or devices that have been approved by your organisation, and keep the number of copies to a minimum. ● Always exercise particular care when storing or accessing names and contact details, and ensure that you are compliant with your organisation's policies and with data protection legislation. ● In the office: ○ Keep your desk clear of hard copy information not in use. ○ Store in an opaque folder or container when not in use. ○ Can be accessed in parts of the building which are accessible to the public ● In public: ○ Store in an opaque folder, bag, or container which can be secured to prevent accidental loss. ○ Can be accessed, but be aware of whether you can be overlooked by unauthorised individuals, such as members of the public. ● Working remotely:	**Storage & Access** ● Only print on corporate systems or devices that have been approved by your organisation, and keep the number of copies strictly to what is required. ● In the office: ○ Keep your desk clear of hard copy information not in use. ○ Store in an opaque folder or container when not in use, and under lock and key when unattended. ○ Use office furniture/physical security equipment that can be securely locked. ○ Do not access in parts of the building which are accessible to the public. ○ Risk assess before accessing in high-traffic areas, such as canteens or 'drop in' workspaces. ● In public: ○ Store in an opaque folder, bag or container, which can be securely fastened to prevent accidental loss. ○ Do not access where you can be overlooked. ○ Do not access OFFICIAL-SENSITIVE information in public. ● Working remotely: ○ Store as securely as possible (in a discreet, opaque container and or/lock and key). ○ Keep out of sight when not in use. ○ Do not access where you can be overlooked. ● Mark all OFFICIAL information with the -SENSITIVE marking in the header and footer.

	○ Store in a discreet, opaque container. ○ Keep out of sight when not in use. ○ Can be accessed in shared spaces, but be aware of whether you can be overlooked ● Avoid taking hard copy documents out of the office unless there is a clear business need. ● Where possible, mark all information with “OFFICIAL” in the header and footer. Local organisational policy may override this requirement.	

	Transportation ● Moving physical assets by hand: ○ Use a single sealed opaque cover. ● Moving physical assets by courier/post domestically: ○ Include return address, never mark classification on envelope. ○ Use a reputable commercial courier. ● Moving physical assets overseas (by hand or post): ○ Trusted hand under a single cover. ○ Use a reputable commercial courier's trackable service. ● Check with your security team if you are moving bulk personal data.	**Transportation** ● Moving physical assets by hand: ○ Single sealed opaque envelope/cover. ○ Do not read in public. ● Moving physical assets by courier/post domestically: ○ Include a return address and never mark the classification on the envelope/cover. ○ Use a recorded mail service or reputable commercial courier service. ● Moving physical assets overseas (by hand or post): ○ Trusted hand using opaque double envelopes/packaging. ○ Use a reputable commercial courier's 'track and trace' service. ○ Seek authorisation from the information creator before sending overseas.

	Destruction: ● Do not dispose of information of any classification at home or in public bins; it should be retained securely at home before being taken into the office for disposal. This requirement can be overridden for permanent homeworkers by local organisational policy (set by an SA/SSA or Head of Security); that policy must include guidance on acceptable disposal e.g. using a cross-cutting shredder. SA/SSAs or Heads of Security may also extend this override to non-permanent homeworkers during emergencies, such as a pandemic. ● Only dispose of information in the office using the correct disposal method mandated by your organisation, such as using a confidential waste bin or a shredder.	**Destruction:** ● Do not dispose of OFFICIAL information marked -SENSITIVE at home or in public bins; it should be retained securely at home before being taken into the office. This requirement can be overridden for permanent homeworkers by local organisational policy (set by an SA/SSA or Head of Security); that policy must include guidance on acceptable disposal e.g. using a cross-cutting shredder. SA/SSAs or Heads of Security in HMG organisations may also extend this override to non-permanent homeworkers during emergencies, such as a pandemic. ● Only dispose of information in the office using the correct confidential waste bin or shredder, as defined in the organisation's local policy.

Electronic information	**Storage:** ● Can be saved into shared areas on corporate systems. ● Follow your department's information management principles (including the use of naming conventions) for saving assets to shared drives. ● Where possible, mark all information with "OFFICIAL" in the header and footer. Local organisational policy may override this requirement.	**Storage:** ● Minimise multiple copies on local systems as far as practically possible (e.g. a team should use a single shared copy rather than saving multiple copies in offline folders on their device). ● Only save to a folder if you are confident that all those with access to that folder have need-to-know for the information. ● You should mark all information with "OFFICIAL-SENSITIVE" in the header and footer. ● Follow your organisation's information management principles (including the use of naming conventions) when saving information to shared drives.
	Accessing OFFICIAL information electronically: ● In the office: can be accessed in parts of the building which are accessible to the public ● In public: can be accessed, but be aware of whether you can be overlooked by unauthorised individuals, such as members of the public. ● If working remotely: can be accessed in shared spaces, but be aware of whether you can be overlooked.	**Accessing OFFICIAL information marked -SENSITIVE electronically:** ● In the office: ○ Do not access in parts of the building which are accessible to the public. ○ Risk assess before accessing in high-traffic areas, such as canteens or 'drop in' workspaces. ● In public: do not access where you can be overlooked ● Working remotely: do not access where you can be overlooked.

	Sharing OFFICIAL information electronically (via corporate approved channels): ● Can be shared beyond the original distribution list based on need-to-know. ● Authorisation to share information is not required from the information creator. ● Include any additional handling instructions in the subject line or use electronic labelling.	**Sharing OFFICIAL information marked -SENSITIVE (via corporate approved channels) electronically:** ● Information can be shared with individuals outside of your organisation on a strict need-to-know and need-to-share basis. Local organisational policy may also mandate that you seek authorisation from the information creator. ● Include the handling instruction in the subject line or use electronic labelling. ● For RECIPIENTS ONLY information: ○ Include the descriptor in the subject line or using an electronic label. ○ Only share it beyond the original distribution list where necessary and after receiving formal approval from the information creator, and keep them carbon copied (cc'd) on any onward distribution. Blind carbon copy (bcc) should be avoided when using this marking. ○ Only distribute it to named individuals or to a shared inbox if you know who has access to it. Avoid sending to a group email inbox unless all the recipients have a need-to-know.