Guidance 1.7: Frequently Asked Questions

How does the updated system work?

1. The updated GSCP defines the system for the secure handling of HMG information across the three classification tiers: OFFICIAL, SECRET and TOP SECRET. Additional markings (descriptors and handling instructions) have been updated and can be applied within these tiers. These markings are distinct from classifications and are used to signpost the nature of, or apply additional sharing controls to information within a tier. There is also greater guidance for remote working at OFFICIAL and SECRET, in light of increased hybrid working across government.

What are the new handling instructions at OFFICIAL?

2. Standardised markings for commonly-used handling instructions within the OFFICIAL tier have been introduced, such as ‘RECIPIENTS ONLY’, ‘HMG USE ONLY’, ‘EMBARGOED UNTIL __’ etc.

3. A centralised list of handling instructions and descriptors alongside their definitions can be found within the full policy on GOV.UK. HMG departments, agencies and public bodies (hereinafter HMG organisations) are able to define additional handling instructions. You should check your organisational policy for more information.

Can I share OFFICIAL information with other HMG organisations and what is the process?

4. Information can be shared at OFFICIAL with other HMG organisations on a need-to-know basis. Access to OFFICIAL information should always be no wider than is deemed necessary for business needs and should be risk-based. Permission to share is not required by the information creator, except where restrictive additional markings apply e.g. where the “RECIPIENTS ONLY” handling instruction has been used.

How do I know that the information is classified at OFFICIAL if there isn’t a marking on the document?

5. Any information that is created, processed or moved (sent and received) as a part of your work for HMG falls within the GSCP and is OFFICIAL by default (even if no visible marking is present) unless it is classified at a higher tier. The information creator is responsible for assessing the expected threat profile of a piece of information, and the potential impact of a compromise, to determine the right marking and controls to apply.

Has the use of OFFICIAL-SENSITIVE changed?

6. The updated GSCP clarifies what sort of OFFICIAL information should use the marking -SENSITIVE. Further information about applying the -SENSITIVE marking can be found in the main policy document and Guidance 1.1: Working at OFFICIAL.

7. A clearer policy definition of the type of information which should be marked -SENSITIVE is intended to reduce user confusion and improve consistency around its application. This should make it easier for HMG organisations to apply consistent controls to OFFICIAL material marked -SENSITIVE with a focus on reducing the risk of accidental compromises (e.g. via loss of hard copies or being overheard in a public space) and ensuring that the need-to-know is properly considered.

Are there any rules on filenames for OFFICIAL documents?

8. You should check your HMG organisation's information management principles (these are usually found on your staff intranet) for more details on local naming conventions.

Can I use colour coding to indicate a document's sensitivity?

9. Information creators should not colour code the classification marking in the header or footer to indicate the sensitivity of a piece of information. However, you should consider printing SECRET documents on pink coloured paper and TOP SECRET documents on yellow coloured paper in certain environments to make them easier to recognise (in conjunction with your organisation's accessibility and sustainability guidance).

How do I ensure that I can restrict access to the file electronically?

10. Once stored, you can check who has access to the document via your local IT system, and access should be managed on a need-to-know basis. In addition to managing who has access to the information, you should check if any handling instructions are needed. For detailed instructions on how to

manage information on shared drives please refer to your information management policy.

Has the policy changed if I'm working with international partners?

11. No. If HMG organisations have a requirement to provide classified information to an international partner, or hold international classified information provided by partners, they must follow the International Classifications Policy. This document is available from the Government Security Group.

How do I evaluate the effects of aggregation on OFFICIAL documents?

12. For more information about how to evaluate the effects of aggregation see Guidance 1.5: Considerations for Security Advisors on GOV.UK. Users should always check with their organisation's security team if they are unsure about how to proportionately protect an aggregated dataset in a given case.

How do I downgrade a document to OFFICIAL?

13. The sensitivity of information can evolve through its life cycle e.g. documents detailing information about a closely-held sensitive public announcement might be classified as SECRET until announced, but would be OFFICIAL from the moment of announcement. It is the information creator's responsibility to reclassify and remark the material if the context around an information asset has changed.

14. It also is the responsibility of the information creator to inform recipients if classified information they have provided has been downgraded, unless they have applied a clear marking or instructions in writing. Without clear guidance and evidence to the contrary, it should *not* be assumed that documents produced with the same title (or a similar title), but with differing classifications, are the same - and they should be handled in line with the relevant classifications and additional markings.

Do I need to inform an Information Asset Owner (IAO) every time I create an OFFICIAL document?

15. You do not need to inform your IAO every time an OFFICIAL document is created. However, all IAOs across government have a responsibility to: understand what information is held by their unit or directorate; what is added and what is removed; how information is moved and transferred/shared; and, who has access to it and why. This means that they need to: understand and address risks to their information; ensure that such

information is appropriately protected and marked; is fully used within the law: and, used in compliance with all legal requirements such as the Data Protection Act 2018 and UK GDPR.

How do I know who the IAO is for a piece of OFFICIAL information?

16. In the first instance, you should ask through your line management chain. Some organisations may choose to publish a list of staff designated as IAOs on their intranet.

How do I know that I’ve correctly classified a document as OFFICIAL?

17. The information creator is responsible for assessing the expected threat profile of a piece of information, and the potential impact of a compromise, to determine the right classification, marking and controls to apply. Information classification tiers are used to indicate the sensitivity of the asset in terms of the likely impact resulting from compromise, loss or misuse, and provide baseline controls to protect against distinct threat profiles, which reflect the broad range of threat actors typically expected at that tier. If you’re unsure about whether you’ve correctly classified a document, you should contact your organisation’s security team.

How can I locate the information creator of a document classified as OFFICIAL?

18. In the first instance, you should check the file description or document details. If you're still unable to locate the information creator you should contact your IAO. If the information creator has left the organisation, you should contact the business unit or directorate where the information originated from.

What recommended security behaviours should I apply when handling HM Government information and data to ensure it stays secure?

19. The updated policy includes a list of baseline security behaviours for each classification tier - see: Guidance 1.1: Working at OFFICIAL; Guidance 1.2: Working at SECRET; and, Guidance 1.3 Working at TOP SECRET.

Who does the updated system apply to?

20. HMG organisations should apply this policy and ensure that consistent controls are implemented throughout their public sector delivery partners (i.e. non-departmental public bodies and arm’s length bodies) and their wider supply chain.

21. Any information that is created, processed or moved (sent and received) as a part of your official duties falls within the GSCP. Everyone who works in or with HM Government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not.

Where can I find more information about applying the updated policy?

22. More information about the updated policy is likely to be available on your organisation's staff intranet or by seeking advice directly from your security team.

When should I start implementing the updated policy?

23. The updated GSCP will come into force on 30th June 2023. A commercial implementation window of 12 months will come into effect from this date until the 29th June 2024.The classification of historic information only needs to be updated in line with the GSCP update if it is redrafted/replaced. Your organisation may define an update programme, where it has been decided to be more efficient to do so.