Cabinet Office

Government Security Classifications Policy

5 August 2024

Executive Summary

The Government Security Classifications Policy (GSCP) provides an administrative system for HM Government (HMG) and our partners to protect information assets appropriately against prevalent threats.

The administrative system uses three classification tiers (OFFICIAL, SECRET and TOP SECRET) that each provide a set of protective security controls and baseline behaviours, which are proportionate to the potential impact of a compromise, accidental loss or incorrect disclosure AND the level of interest expected from threat actors. The protective controls must be balanced with the need for utilising those assets to support the effective conduct of government business.

Any information that is created, processed or moved (sent and received) as a part of your work for HMG falls within the GSCP.

Cabinet Office
2024

Contents

List of Acronyms

Included is a list of acronyms used throughout the GSCP and its accompanying guidance documents:

BPSS - Baseline Personnel Security Standard
CIK - Crypto Ignition Key
CNI - Critical National Infrastructure
CSE - Catalogue of Security Equipment
DPA - Data Protection Act 2018
DV - Developed Vetting
FOI - Freedom of Information
FOIA - Freedom of Information Act 2000
GCSO - Government Chief Security Officer
GDPR - UK General Data Protection Regulation
GSB - Government Security Board
GSCP - Government Security Classifications Policy
GSG - Government Security Group
HMG - His Majesty's Government
HR - Human Resources
IAO - Information Asset Owner
IT - Information Technology
LPP - Legal Professional Privilege
NATO - North Atlantic Treaty Organisation
NCSC - National Cyber Security Centre
NPSA - National Protective Security Authority
OSA - Official Secrets Act 1989
PDF - Portable Document Format
PDR - Protected Document Registry Book
PRA - Public Records Act
SA - Security Advisor
SC - Security Check
SCS - Senior Civil Servant
SSA - Senior Security Advisor
UK NSA - UK National Security Authority

Key Principles

1. The GSCP describes HMG's administrative system for the secure, timely and efficient sharing of information. It is not a statutory scheme but operates within the framework of domestic law (see Annex A).

2. This policy should be read in conjunction with organisations' local information security and classifications policies, which will set out risks, controls and processes relevant to their business context.

3. Within each classification tier, information should be protected to the baseline security controls framework outlined within the GSCP, wherever it is collected, stored, processed or shared across HMG and with the wider public sector and external partners. This consistency is essential to provide the confidence that underpins effective information sharing and interoperability between organisations.

4. All HMG information should be clearly marked with a classification tier. However, there are a wide variety of operational settings where marking OFFICIAL information would either be inappropriate or not possible. Local organisational policy set by an SA/SSA or Head of Security may therefore override this requirement for OFFICIAL information, which has no additional marking.

Principle One: ALL information that HMG needs to collect, store, process, generate, dispose or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

5. This policy provides detail on the security classifications which are applied to HMG information and indicates its sensitivity (in terms of the likely impact resulting from compromise, loss or misuse).[1] They also provide a minimum set of security controls and baseline behaviours to protect against distinct threat profiles, which reflect the broad range of threat actors typically expected at that tier. The three classification tiers are: OFFICIAL, SECRET and TOP SECRET.

[1] For the purpose of this policy the term "information" can also include physical assets which can hold a security classification due to the information they can reveal. Physical Assets are not normally marked but their security classification shall be identified in a Security Aspects Letter, Security Grading Guide or other documentation.

6. The baseline behaviours and security controls that accompany each of the classification tiers detail means by which information is protected. The baseline behaviours are primarily focused at information users; security controls at Security Advisors and their security teams.

7. The baseline behaviours (found in Guidance 1.1: Working at OFFICIAL; Guidance 1.2: Working at SECRET; and, Guidance 1.3: Working at TOP SECRET) provide a set of recommended behaviours for users on how to handle HMG information, to minimise the risk of information being compromised. Each set of behaviours is cumulative and provides the foundation for higher levels.

8. For each classification there is a minimum set of security controls. These are outlined in the security controls table (found in Guidance 1.5: Considerations for Security Advisors). The controls table forms a minimum set of measures that provide the basis for the development of local security controls to reduce the risk of information assets being compromised. Each set of controls is cumulative and provides a foundation for higher levels.

9. HMG information should be managed in line with the 'Code of Practice' outlined in Section 46 of the Freedom of Information Act 2000 (FOIA). This sets out a framework for the keeping, management and the destruction of information.

Principle Two: Organisations may apply additional security controls and behaviours above the baselines outlined in this policy (but not below), in line with the organisation's risk appetite.

10. The organisation's Senior Security Advisor (SSA)/Security Advisor (SA) or Head of Security own local policies and should ensure that this information is readily available in an easily accessible location for staff, such as on the organisation's local intranet. Any additional organisational controls not addressed in this policy, or covered in sufficient detail, should be clearly set out in local policies approved by the organisation's SSA/SA or equivalent.

11. SSA/SAs or the Head of Security should conduct assurance activities to test compliance with the GSCP, and inform continuous improvement activities.

12. To aid effective information sharing between organisations, when information has additional controls and processes (beyond those outlined in the GSCP) applied, the recipient is expected as a minimum to protect the information to

the baseline outlined in the policy, unless notified that they must go beyond this by the sender.

Principle Three: Everyone who works with 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 and/or share, irrespective of whether it is marked or not, and must be provided with appropriate training. Individuals are accountable for their own security decisions.

13. Accidental or deliberate compromise, loss or misuse of HMG information may lead to damage and can constitute a criminal offence. Damage in this case can be as extreme as causing a threat to life to individuals, or serious harm to the UK (see Annex B).

Principle Four: Information should be protected proportionately to the impact of compromise and the capability and intent of threat actors likely to seek that information. Access to information must ONLY be granted where there is assurance that appropriate security controls (personnel, physical, procedural and technical) are in place.

14. OFFICIAL information that has been cleared for public release or disclosure, or is freely available in the public domain, requires no additional assurance and it would be disproportionate to protect it with security controls.

Principle Five: Information should be handled and distributed based on a genuine need-to-know, balanced with the need-to-share (as defined in the glossary), dependent on the sensitivity of the information.

15. The need-to-share is underpinned by a need-to-know i.e. the potential recipient must have a legitimate need to use the information. In any circumstance where a need-to-share has been identified, the information must be protected in line with the controls and necessary approvals for its classification.

16. The need-to-share principle recognises that the information creator or user may identify situations (informed by the information's sensitivity and risk of compromise) where sharing information outside the original circle of

knowledge will create value, help achieve organisational aims, support the efficient conduct of the organisation's business or be as a result of a successful Freedom of Information (FOI) request.

Principle Six: Information received from or exchanged with external partners MUST be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

17. The policy applies equally to assets entrusted to HMG by others, such as foreign governments, international organisations, NGOs and private individuals.

18. Where specific reciprocal security agreements / arrangements are in place with foreign governments or international organisations, equivalent protections and markings must be recognised and any information received must be handled with AT LEAST the same degree of protection as if it were UK information of equivalent classification.

19. Where no relevant security agreements / arrangements are in place, information or other assets received from a foreign country, international organisation or a NGO must at a minimum be protected to an equivalent standard as that afforded to HMG OFFICIAL assets, although higher classifications may be appropriate.

20. The need-to-know principle must be strictly enforced for access to international partners' information.

21. How the UK provides classified information to international partners, and how HMG is required to protect international classified information it receives from those partners, is addressed in a specific policy set by the Government Security Group (GSG). This policy sets out special handling processes and requirements which ensures that UK classified information is protected to acceptable standards by partners. This policy also sets out how the UK protects its partners' classified information to agreed standards (which can be subject to external audit by partners). Teams and units that routinely provide UK classified information and/or receive international classified information from partners should seek guidance from their SSA/SA, who in turn can seek advice from the UK National Security Authority (UK NSA) in GSG.

Definitions for OFFICIAL, SECRET and TOP SECRET

OFFICIAL
Definition: The majority of information that is created, processed, sent or received in the public sector and by partner organisations, which could cause no more than moderate damage if compromised and must be defended against a broad range of threat actors with differing capabilities using nuanced protective controls. Aggregated data sets of OFFICIAL information may warrant additional controls (see Guidance 1.5: Considerations for Security Advisors).
Threat Profile: The threat profile for the OFFICIAL classification tier anticipates a need to defend against a broad range of threat actors, which may include, but is not limited to; staff who pose insider risk, hacktivists, pressure groups, unauthorised leaks to the media, competent hackers, state actors and criminal individuals and groups. This model does not imply that information within the OFFICIAL tier will not be targeted by some sophisticated and determined threat actors (including Foreign Intelligence Services), who may deploy advanced capabilities. It may be rather that a risk-based decision has been taken not to invest in controls to assure protection against those threats i.e. proportionate rather than guaranteed protection. Even whilst not seeking guaranteed protection, OFFICIAL can still be made a hard target through using proportionate risk-based decisions, to thwart threat actors that use well-known techniques, whilst also aiming to detect those using advanced capabilities.
Working at OFFICIAL For policy guidance on working at OFFICIAL including its application and associated baseline security behaviours for users, see Guidance 1.1: Working at OFFICIAL.
Risks of a compromise:

In most cases there are limited to no negative consequences if OFFICIAL information is compromised. However, in some circumstances when OFFICIAL information contains sensitive information and is marked -SENSITIVE, its unintended disclosure or compromise can lead to moderate damage (including to the UK's longer-term strategic/economic position) and in exceptional circumstances it could lead to a threat to life.

Due to the wide-ranging sensitivity of different information that sits within this tier, the effect of an accidental or deliberate compromise at OFFICIAL can be broad, but would likely result in any of the following:

Life and safety

a. Typically causes no more than moderate, short-term harm to an individual or a group of people's safety. However, in some exceptional circumstances, the compromise of more sensitive OFFICIAL information could lead to a threat to life.
b. Causes no more than moderate damage to the UK's ability to plan for potential future emergencies ('emergency' is used in the sense defined by Section 1 of the Civil Contingencies Act 2004) or serious incidents.
c. Causes no more than limited disruption to the smooth delivery of an emergency or serious incident response (but not to the extent that it impairs the effectiveness of that response).

International relations

d. Causes no more than moderate, short-term damage to relations with friendly governments; or damage to the international reputation of the UK or a friendly country.

Military operations

e. Causes no more than moderate, short-term damage to the operational effectiveness of UK or allied forces' military operations.

Prosperity

f. Causes no more than moderate, short-term damage to the commercial, economic and financial interests of UK or local economies.
g. Causes no more than moderate, short-term damage to the effectiveness or reputation of organisations.

Security and Intelligence

h. Causes no more than moderate delays in the ability to investigate or prosecute serious organised crime.
i. Causes no more than moderate damage to the security and resilience of critical national infrastructure (CNI) assets.

Vetting requirement

No national security vetting is required to access OFFICIAL information but all HMG staff and contractors must undergo a BPSS pre-employment check (or equivalent).

Contracting Authorities should continue to ensure all contractors that have access to HMG information continue to follow the vetting requirements outlined in Contractual Process 2018.

SECRET

Definition:

Very sensitive information that requires enhanced protective controls, including the use of secure networks on secured dedicated physical infrastructure and appropriately defined and implemented boundary security controls, suitable to defend against highly capable and determined threat actors, whereby a compromise could threaten life (an individual or group), seriously damage the UK's security and/or international relations, its financial security/stability or impede its ability to investigate serious and organised crime.

Threat Profile:

The threat profile for SECRET anticipates the need to defend against sophisticated, well-resourced and determined threat actors with higher levels of capabilities than would be typical for the OFFICIAL tier. This includes, but is not limited to: capable state actors; sophisticated state sponsored actors such as cybercrime groups; some serious organised crime groups; and, staff who pose insider risk. Proportionate technical capabilities, user behaviours and security controls will be used to protect information and services from compromise by these actors, including from targeted and bespoke attacks.

Working at SECRET

For policy guidance on working at SECRET including its application and the associated baseline security behaviours for users, see Guidance 1.2: Working at SECRET.

Risks of a compromise:

The effect of accidental or deliberate compromise would be likely to result in any of the following:

Life and safety

a. Directly threaten an individual's life, liberty or safety (from capable threat actors).
b. Causes major impairment to the UK's ability to effectively plan for potential future emergencies or serious incidents.
c. Impede the UK's response to emergencies or serious incidents.

Military operations

d. Causes serious damage to the operational effectiveness or security of UK or allied forces so as to make it impossible to deliver military tasks or render current or future capabilities, or installations, unusable.

International relations

e. Causes serious damage to the international reputation of the UK or a friendly country.
f. Causes serious damage to the relations with friendly countries, resulting in formal protest or sanction.

Prosperity

g. Causes serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.

Security and intelligence

h. Causes serious damage to the operational effectiveness of highly valuable security or intelligence operations.
i. Causes major impairment to the ability to investigate or prosecute serious organised crime.

j. Causes major impairment to the ability to address (i.e. deter, respond to, investigate or prosecute) terrorism, espionage, or other activities that undermine UK national security or parliamentary democracy.
k. Causes serious damage to the security and resilience of CNI assets.
l. Otherwise cause serious damage to UK national security.

Vetting requirement

Security Check (SC) for regular or uncontrolled access.

TOP SECRET

Definition:
Exceptionally sensitive information assets that directly support or inform the national security of the UK or its allies AND require an extremely high assurance of protection from all threats with the use of secure networks on highly secured dedicated physical infrastructure, and robustly defined and implemented boundary security controls.

Threat Profile:
The threat profile for TOP SECRET reflects the highest level of capability deployed against the most sensitive information and services. It is assumed that advanced hostile state actors will prioritise compromising this classification of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated.

Working at TOP SECRET
For policy guidance on working at TOP SECRET including its application and the associated baseline security behaviours for users, see Guidance 1.3: Working at TOP SECRET.

Risks of a compromise:
The effect of accidental or deliberate compromise would be likely to result in any of the following:

Life and safety:

m. Could lead to loss of human life.

n. Causes exceptionally grave, long-term, or systemic impairment to the UK's ability to effectively plan for potential future emergencies or serious incidents.

o. Threaten directly the UK's ability to respond to an ongoing emergency.

Military operations

p. Causes exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Outcomes.

International relations

q. Raise international tension.

r. Causes exceptionally grave damage to relations with friendly nations or those we cooperate with closely.

Prosperity

s. Causes long term damage to the UK economy.

Security and Intelligence

t. Threaten directly the national security or internal stability of the UK or friendly nations.

u. Causes exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

v. Causes major, long-term impairment to the ability to investigate or prosecute serious organised crime.

w. Causes major, long-term impairment to the ability to address (i.e. deter, respond to, investigate or prosecute) terrorism, espionage, or other activities that undermine UK national security or parliamentary democracy.

x. Otherwise cause major, long-term harm to UK national security.

Vetting requirement

Developed Vetting (DV) for regular or uncontrolled access.

Additional Markings

What are Additional Markings?

22. Security classifications are the principal means of indicating the sensitivity of a particular asset and the requirements for its protection. Additional markings can be added in conjunction with a classification to indicate the nature or source of the information, or to limit access to specific user groups. Additional markings indicate where additional protective controls or security behaviours are required to protect the information.

23. There are several different types of additional markings, including: the -SENSITIVE marking, handling instructions, descriptors, codewords, prefixes and national caveats.

24. Information creators should apply additional markings to help users understand information sensitivities and specific restrictions on information sharing. Users must be given by their security teams guidance on how to mark and protect information with additional markings.

Applying the -SENSITIVE marking

25. The most common additional marking is the use of -SENSITIVE to mark OFFICIAL information. The -SENSITIVE marking should be applied to OFFICIAL 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. A compromise of OFFICIAL information or material marked -SENSITIVE is likely to cause moderate damage to the work or reputation of the organisation and/or HMG and must be marked with the -SENSITIVE marking. This marking should be applied immediately after the OFFICIAL classification, and before any other handling instructions or descriptors.

26. Further information about how the -SENSITIVE marking should be applied to OFFICIAL information can be found in Guidance 1.1: Working at OFFICIAL.

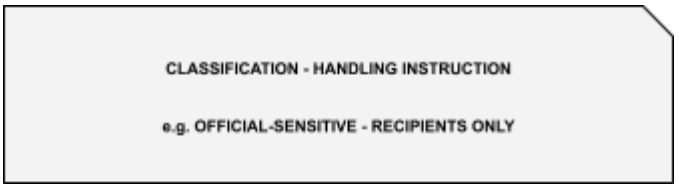
Handling Instructions

Within a classification tier, handling instructions can also be used to give a more detailed picture of the information's sensitivity and how it should be appropriately handled. Handling

instructions do not change the information's classification as the threat profile is the same, nor do they offer additional technical protections; they just provide more detail around how information should be handled, how widely it should be disseminated and how it should be protected.

A centrally defined list of handling instructions is included below.

The preferred format for Handling Instructions is:



Handling Instructions	**Definition**
RECIPIENTS ONLY *Can be applied to: OFFICIAL-SENSITIVE, SECRET and TOP SECRET* *(Previously also applied to OFFICIAL)*	This handling instruction is reserved for a small subset of particularly sensitive information that carries high risks associated with compromise. The information creator should apply the RECIPIENTS ONLY marking to indicate that the information must be handled on a strict need-to-know basis by select named individuals. The information creator should have strict control over who the information gets shared with beyond the original recipients. Meeting attendees should seek authorisation from the meeting chair before briefing to, or discussing with, other colleagues not on the distribution list. Where this is not possible, such as for large meetings, the chair may waive this requirement but should notify meeting attendees that this information should only be distributed further on a strict need-to-know basis.

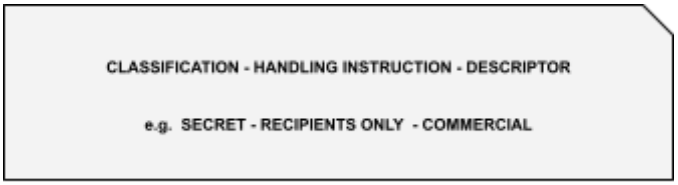
	When this handling instruction is used, you should also use a meeting room where you will not be overheard, and consider banning mobile phones and other smart electronic devices (such as smart watches) from the meeting. The need-to-share without authorisation from the information creator is not justified due to the risks of compromise of this information. Use of the RECIPIENTS ONLY marking is strongly recommended, but is at the organisation's discretion. Users should consult their local organisational policy.
FOR PUBLIC RELEASE *Can be applied to: OFFICIAL only* *FOR PUBLIC RELEASE can not be used in conjunction with the -SENSITIVE marking.*	OFFICIAL information which can be distributed without restriction, because it has been cleared for publication, is already in the public domain or is subject to release in accordance with the FOIA or the Public Records Act 1958. The information is of low sensitivity and there is a need-to-share the information with the general public. Before publication, ensure that appropriate quality assurance checks are undertaken (including, if appropriate consulting your organisation's press office and legal team).
[INSERT ORGANISATION(S) NAME] USE ONLY *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET, TOP SECRET*	Information that should only be shared within the named organisation(s). Users should seek permission from the information creator before sharing outside the named organisation(s).
HMG USE ONLY *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET*	Information that should only be shared with other HMG departments; not with external partners.

EMBARGOED *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE) and SECRET alongside clearly indicated subsequent handling instructions for reclassification after an identified period.*	Information that is only sensitive for a specific period of time and whose sensitivity will be reduced at the end of that period. Where this marking is used, the relevant time and date, and subsequent handling instructions, must be clearly indicated as close as possible to the classification marking.
Note: Your organisation may define additional handling instructions, so you should check your organisation's policy for more information.	

Descriptors

Descriptors are terms applied by users to easily identify certain categories of information with special sensitivities and highlight additional access restrictions. Descriptors are <u>not</u> additional classifications and do <u>not</u> need to be applied to all documents. A centrally defined list of Descriptors is included below.

Descriptors go after the classification, and after the handling instruction (if there is one) in the following format:



PERSONAL DATA *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET* and *TOP SECRET*	Information relating to a living individual who is identified, or can be indirectly identified, by the information. Users should ensure that they are aware of legal obligations relating to the processing of personal data, and any additional security behaviours and controls required by their organisation for related personal data tasks (in particular, when processing aggregated personal

	data), beyond the local baseline applied for the relevant classification level. There are additional legal obligations that apply for the processing of special category data, as defined by the UK GDPR and Data Protection Act 2018. The Personal Data section of "Further Considerations for Users" (below) provides additional guidance. The HR/Management descriptor should be applied to workforce information where individual staff are not identifiable. It can also be applied to information relating to identifiable individuals (such as employment contracts, performance assessments, etc), but considerations relating to the processing of personal data will continue to apply.
LEGAL PROFESSIONAL PRIVILEGE (LPP) *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET, TOP SECRET*	Information that exists for the purpose of giving or receiving legal advice and is contained in confidential communications passing between a client (e.g. a business area) and the client's lawyer (e.g. a member of the Legal Directorate or external counsel); or, confidential communications between a lawyer and their client, or between either of them and a third party, that relate predominantly to litigation which is actual or pending at the time of the communication.
LEGAL *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE)*	Information that relates to active or potential criminal or civil proceedings. If the information in question includes protected legal advice, use the LPP descriptor (see above) instead.
MARKET SENSITIVE	Information that is not public and could have a material impact on financial markets i.e. could move market prices. This includes micro-level information on

Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET, TOP SECRET	the pricing of financial instruments or the activities of specific market participants. It also covers macro-level information such as Bank of England policy initiatives which could influence market prices. A subset of this information will comprise 'inside information' as defined by the Market Abuse Regulation (Article 7).
COMMERCIAL *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET, TOP SECRET*	Information that may be commercially damaging to your organisation or to a commercial partner if improperly accessed, or which is subject to terms of commercial confidentiality. If the information could have a material impact on financial markets, use the MARKET-SENSITIVE descriptor (see above) instead.
HR / MANAGEMENT *Can be applied to: OFFICIAL (including OFFICIAL information marked -SENSITIVE), SECRET AND TOP SECRET.*	Information relating to the workforce, including sub-groups, where individuals are not identifiable (see Personal Data descriptor). OR Information relating to individual staff who are directly or indirectly identifiable (such as employment contracts, performance assessments, etc). In this instance, the user considerations relating to the processing of personal data continue to apply. Users should ensure that they are aware of any additional security behaviours and controls required by their organisation for the internal processing of HR/Management information; in particular, where individual staff permission is required in advance.

Note: Some organisations may require specific descriptors to suit their business needs. Users should refer to their local policy before using any of the centrally defined descriptors. If in doubt about the meaning or handling of a descriptor, always check with the information creator and/or your security team.

Codewords

Codewords provide security cover for a particular asset or event. A codeword is a single word expressed in CAPITAL letters. They are most commonly applied to SECRET and TOP SECRET assets. Codewords are centrally allocated; please contact your SSA/SA if you require one for an asset at any tier.

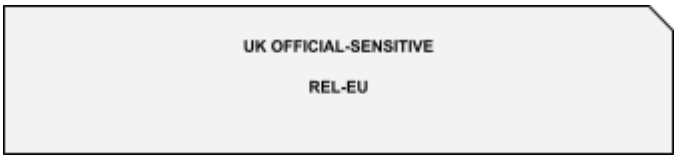
Codewords go after the classification and the handling instruction. Please see below for an example:

Prefixes and National Caveats

Specific markings may be used either to indicate the provenance of sensitive information or as a means to control dissemination.

a. UK Prefix - ALL assets sent to foreign governments or International Organisations (e.g. the North Atlantic Treaty Organisation (NATO)) must be marked with a UK prefix. The UK prefix is added to minimise the risk that HMG classified assets could be disclosed under an international partner's public disclosure legislation. In addition, a handling instruction setting out the conditions for release may also be added to the information. An example of the application of both the prefix and handling instruction follows:

b. REL EU - Under the UK's security relationship with the European Union any UK classified information provided to an EU institution must, in addition to the UK prefix described above, include a releasability marking 'REL EU'. An example follows:

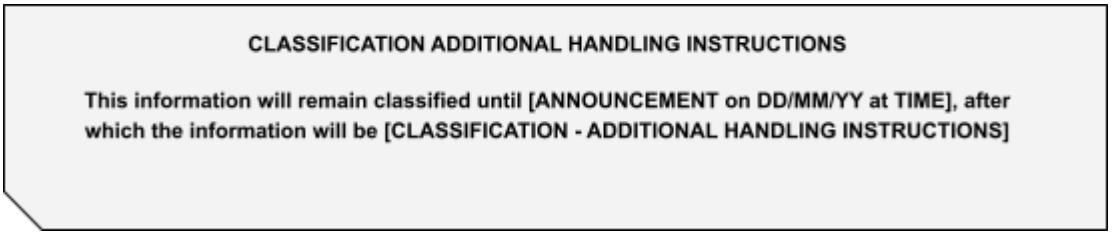


National Caveats are used to designate assets of particular sensitivity to the UK or where dissemination must be restricted to individuals from specific foreign nations. National Caveats (e.g. UK EYES ONLY) can only be applied to SECRET and TOP SECRET assets.

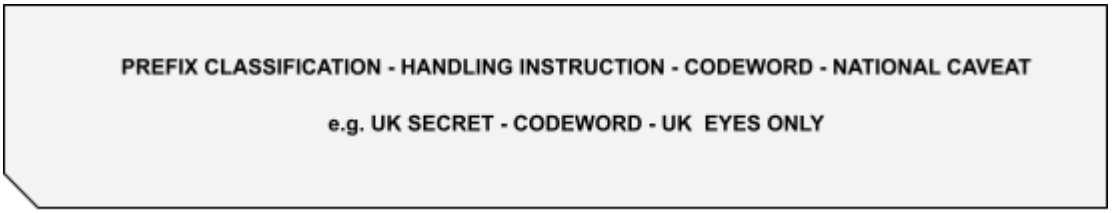
UK EYES ONLY *(Also other National Caveats,* for example*: UK/US EYES ONLY, FIVE EYES ONLY. If multiple National caveats are applied, they must be placed in alphabetical order).* *Can be applied to: SECRET, TOP SECRET*	Information that is of particular sensitivity to the UK or that should only be shared with nationals of the country or countries listed in the handling instructions. Unless explicitly named, information bearing such a marking must not be sent to foreign governments, overseas contractors, international organisations or released to any foreign nationals (either overseas or in the UK) not listed in the National Caveat - without the information creator's consent. N.B. With the exception of British Embassies and Diplomatic Missions or Service units or establishments, assets bearing the UK EYES ONLY National Caveat must only be sent overseas in exceptional circumstances and where access by those with a British nationality can be strictly controlled. This is not a matter of security clearance but one of nationality only.

Additional Instructions

27. All information should, where possible, be marked with a classification, but not all information requires additional markings. The handling instructions included above are the most commonly used, but information creators may choose to provide additional instructions where necessary. For example:



28. If a user decides that all additional markings are required, they should be applied in the following order and format:



Users should check their security team's guidance for any additional handling instructions relevant to their organisation.

Further Considerations for Users

Personal Data

29. The loss or misuse of personal data can have significant implications for affected individuals (including to their personal safety) and for organisations.

30. All personal data is subject to legal obligations. There is not an exhaustive defined list of what constitutes personal data but it covers any information relating to a living, identified or indirectly identifiable person.

31. Due to its sensitivity, there are additional legal obligations relating to a subset of personal data “special category data”. Special category data is legally defined as:

a. personal data revealing racial or ethnic origin;

b. personal data revealing political opinions;

c. personal data revealing religious or philosophical beliefs;

d. personal data revealing trade union membership;

e. genetic data;

f. biometric data (where used for identification purposes);

g. data concerning health;

h. data concerning a person's sex life; and

i. data concerning a person's sexual orientation.

32. Further information on the processing of special category data can be found on the Information Commissioner's Office's website here.

33. Local procedures set by organisations must meet legal obligations and should guide users on any additional security behaviours and controls that the organisation requires for specific data activities, including the preparation of data for public release (such as pre-disclosure checks).

34. Data controllers and users should give appropriate consideration to their evolving responsibilities throughout the data lifecycle. Personal data held by an organisation cannot automatically be repurposed for alternative uses. It can though be reused in certain circumstances: if the purpose of doing so is compatible with the original purpose of processing the data; if the subject gives consent; or, if the processor has a clear obligation or function set out in law. Data controllers and users should be mindful that individuals may become identifiable when data is used for different purposes or is used in conjunction with other information by a different controller.

35. The processing of aggregated personal data sets requires particular care as aggregation can increase the potential impact of data misuse. For further information on the technical controls that should be applied to aggregated data, please refer to Guidance 1.5 Considerations for Security Advisors.

36. Further guidance on processing personal data is widely available. For example, training is available on Civil Service Learning and local experts, such as data protection leads and legal advisers, can be consulted.

Reclassifying an information asset

37. Only the information creator from the originating organisation can reclassify and/or change the classification of an asset.

38. Information users may challenge the classification of an asset with a reasoned argument. A consideration to reclassify an information asset should consider the right balance between controls to protect information with the need to utilise assets to support the effective conduct of government business (i.e. a need-to-know and need-to-share consideration).

39. In some rare instances (for example, as part of a longstanding contract), you may encounter information that has been classified using the previous Government Protective Marking Scheme (GPMS). If this information is still being processed, the information creator should consider reclassifying the information using the current Government Security Classifications Policy. Further information on the contractual implications of reclassification can be found in Guidance 1.6: Contractors and Contracting Authorities. Historical information held under the Public Records Act 1958 should not be reclassified or amended.

Publication or Disclosure

40. When a sensitive asset is being considered for publication or disclosure, every effort should be made to consult the information creator and/or originating department. It may also be appropriate to consult the organisation's lawyers. This includes disclosure of an asset under the FOIA or transfer to The National Archives for permanent preservation under Section 3 of the Public Records Act 1958 (some material may be subject to a longer retention period where necessary e.g. for national security reasons).

41. Where information has been cleared for publication or disclosure, the information creator and/or originating department should apply the FOR PUBLIC RELEASE handling instruction to the copy of the asset being released to indicate that the information can be shared without restriction, including with the general public. This is to ensure that information users do not employ burdensome and expensive security controls and resources to information where there is no risk, and doing so would impact the effective conduct of government business. Original historical records being released at The National Archives under the Public Records Act must be scrutinised to redact sensitivities that persist and are still protected by FOI exemptions

before they are transferred. However, they should not be defaced with new markings.

Annex A - Legal Framework

42. The GSCP is set by HM Government and operates within the framework of domestic law. This includes:

    a. **Official Secrets Act 1989** (OSA): Damage assessment is a critical element of the OSA. Most of the offences require there to have been a damaging disclosure of information relating to security or intelligence, defence, international relations, crime or special investigation powers, or of confidential information received from a foreign State or an international organisation. With respect to each type of information, the OSA describes the type of damage which has, or would be likely, to flow from an unauthorised disclosure. The OSA also specifies who is capable of committing offences under it.

    b. **Data Protection Legislation**: The handling of personal data must be in compliance with data protection legislation. However, the Data Protection Act 2018 (DPA) contains a number of exemptions to some or all of the data protection principles and to other provisions such as the right of access to personal data. For example, the Act provides an exemption from many of the requirements of the United Kingdom General Data Protection Regulation (UK GDPR) to safeguard national security. But while this exemption is widely drawn, it is only available to the extent that it is required for the purpose of protecting national security. Thus departments and agencies will still be required to assess whether it is possible to address national security concerns and comply with data protection legislation. Whilst the presence or absence of a classification marking is not in itself a deciding factor as to whether an exemption is engaged, it may be a helpful indicator that one might apply. Departments and agencies should also have regard to data protection legislation, including any relevant exemptions, when sharing personal data with other departments and agencies or pursuant to international agreements.

    c. **Freedom of Information Act 2000**: Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each freedom of information (FOI) request must be considered on its own merits and

the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

d. **Public Records Act 1958**: Information selected for preservation may be retained under Section 3(4) of the 1958 Act (as amended) or closed under an exemption provided by the Freedom of Information Act 2000. Any information not selected for permanent retention or required for a business need must be destroyed at the 20 year point. The retention of information beyond this point (i.e. whether for sensitivity reasons or an ongoing business need) must be approved by the Secretary of State for the Department of Culture Media and Sport, as do closures. Decisions over retention or closure are driven by the assessment of residual sensitivities at the time that release is being contemplated.

Annex B - What to do in the event of a compromise of OFFICIAL, SECRET, TOP SECRET information

43. Staff must immediately report any suspected or actual compromise of OFFICIAL, SECRET and TOP SECRET information to their organisation's security team. This includes any loss, theft, uncleared access or tampering involving classified information or assets. Organisations should immediately contact their Data Protection Team and/or Officer if compromised information contains personal data.

44. In the event of a loss outside the workplace or suspected theft of SECRET and TOP SECRET information, staff must call the police and get a crime reference to give to their security team. Staff should also report near-misses to their organisation's security team.

    Other examples of information compromises are:

    c. Accessing information from any device other than one accredited and/or approved by their organisation.

    d. Accessing SECRET or above information without authorisation.

    e. Viewing information or holding SECRET or above conversations outside of designated areas in line with issued organisational guidance.

45. All information users are expected to understand their organisation's breach policy and legal obligations, including under the OSA. Information compromises (whether intentional or not) will be investigated in accordance with the relevant internal policies. Individuals found responsible for compromising information could face disciplinary proceedings, have their security clearances reviewed (and possibly revoked) and, in serious cases, be liable to criminal prosecution.

Annex C - Glossary

Classification Tier	Indicates the sensitivity of the asset in terms of the likely impact resulting from compromise, loss or misuse, AND provides baseline controls and behaviours to protect against distinct threat profiles, which reflect the broad range of threat actors typically expected at that classification.
Compromise	In the context of security, a compromise occurs when a classified asset (including people, property or information) is exposed intentionally or unintentionally to a system, device, or an unauthorised individual without the appropriate security clearance and/or need-to-know and without a legitimate business need (see need-to-share).
Controls	The protective security measures that aim to reduce and manage the risk of assets being compromised.
Delivery Partner (organisation)	A contractor who has a legitimate business need and the necessary clearance to access, store or process government information, and can be trusted to handle the information appropriately.
Descriptors	Descriptors are applied by users to easily identify certain categories or types of information with special sensitivities and highlight additional access restrictions.
Handling Instructions	Markings which are used within a classification tier to provide additional instructions to staff when handling information. They help protect a range of information with varying sensitivity against a classification's broad threat profile.
Identifiable Living Individual	A living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual (Data Protection Act, 2018).
Information Creator	The person who has the authority over the creation or distribution of an information asset, and is responsible for determining the classification, handling, dissemination and disposal of that information.
Information User	The staff, delivery partners and third-party suppliers who process HMG

	information assets, and are personally accountable for handling, disseminating and disposing of the information responsibly in line with HMG policy.
Insider Risk	Risk arising from a person who (knowingly or unknowingly) misuses legitimate access to compromise, or risk compromise, of classified information.
Need-to-know	Access to sensitive information must be no wider than necessary for the efficient conduct of official work, and limited to those with a business need and the appropriate personnel security clearance.
Need-to-share	Information must be shared with those with a legitimate need. Information is only valuable to a user once they have access to it.
Organisation	HMG departments or agencies, public bodies and government contractors who are responsible for accessing, storing or processing government information.
Personal Data	Any information relating to an identified or identifiable living individual (Data Protection Act, 2018).
Security Outcomes	The baseline aims that an organisation must use when developing appropriate and proportionate information, personnel, physical and cyber security controls, to manage risks to an acceptable level within the organisational risk appetite.
Security Risk	A risk arising from a failure to prevent unauthorised and/or inappropriate access to an asset.
Threat Actor	A person/entity/state which has the capability and intent to impact the security of an asset (including people, property or information). Can also be called a malicious actor.

Annex D - Version History

Document Version	Date Published	Summary of Changes
1.0	30 June 2023	• First version published on GOV.UK
2.0	5 August 2024	• Summary of August 2024 update: ○ The RECIPIENTS ONLY handling instruction has been updated. ○ The PERSONAL DATA and HR/MANAGEMENT descriptor definitions have been updated. ○ A new section dealing with Personal Data has been added to Further Considerations for Users. ○ A new paragraph providing guidance on processing legacy information marked under the Government Protective Marking Scheme (GPMS) has been added to Reclassifying an Information Asset. ○ Text relating to the Public Records Act 1958 has been revised.

[inside of back cover – intentionally left blank]

Any enquiries regarding this publication should be sent to us at governmentsecurity@cabinetoffice.gov.uk

This publication is available at www.gov.uk/government/publications

Printed on paper containing 75% recycled fibre content minimum.