CYBER GUIDELINE DOCUMENT

Police Security Classification Guideline

ABSTRACT:
This guidance is to assist members of the policing community of trust to correctly classify and protect information assets in line with UK Government Security Classification Policy.

This guidance in conjunction with the National Policing Community Security Policy (NCSP) and associated documents supports the requirements of the NCSP Information Management standard.

ISSUED	April 2024
PLANNED REVIEW DATE	April 2025
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This guideline is due for review on the date shown above. After this date, this document may become invalid.

Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guidance in conjunction with the National Policing Community Security Policy (NCSP) Framework and associated documents supports the requirements of the Information Management NCSP standard and the UK Government Security Classification Policy.

Introduction

This guidance is to assist members of the community of trust to correctly classify and protect policing data and assets to align with the UK Government Security Classification Policy (GSCP.) This guidance describes the intended implementation of the GSCP across policing.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guidance is to:

Provide members of the community of trust a reference guide to help correctly classify their data, assets and systems that is consistent with the UK Government security classification policy (GSCP.)

Audience

This guidance is for National Policing and its community members.

Scope

1. This guidance applies to all information assets received, edited, processed, stored, archived or disposed of as part delivery policing objectives.
2. Policing information can include in the form of digital, physical, and unrepresented such as ideas, knowledge and thoughts that are intangible.
3. This guidance applies to any member of the policing Community of Trust and applicable third parties to the policing community.

Guidance

Note for the reader: As per the National Policing Community Security Policy direction on information classification, policing is to follow the Government Security Classification Policy. This guidance is extracted directly from that policy, with only minor changes for the intended audience. For full reference to the unabridged UK Government Security Classification Policy please see: Government Security Classifications - GOV.UK (www.gov.uk)

The UK Government Security Classification Policy (GSCP) uses three classification tiers (OFFICIAL, SECRET and TOP SECRET). Each tier provides a set of recommended baseline behaviours and a set of protective controls, which are proportionate to the threat profile for that tier AND the potential impact of a compromise, accidental loss or incorrect disclosure of information held within that tier.

All information that is created, processed or moved (sent and received) by, within, or on behalf of policing falls within scope and must be protected in a manner consistent with the baselines for each classification tier.

Definitions

OFFICIAL: 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.

SECRET: 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.

TOP SECRET: 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.

Baseline Security Behaviours

The guidance outlines the minimum baseline security behaviours users should follow at each classification tier. It covers the baseline behaviours at each tier for the handling (sharing, storage, transport, and destruction) of information in electronic, hard-copy and verbal formats. These baseline behaviours provide protection proportionate to the level of risk.

Government Security Classifications Policy guidance

As taken directly from that policy, with only minor changes for the intended audience. For full reference to the unabridged UK Government Security Classification Policy please see: Government Security Classifications - GOV.UK (www.gov.uk)

Working at OFFICIAL

"OFFICIAL: 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." (GSCP, 2023)

All information that is created or processed by organisations subject to this security classification scheme is OFFICIAL by default, unless it is classified at a higher level. The majority of police information is classified at OFFICIAL and many users will work only at the OFFICIAL tier. Use of this marking is recommended, users should consult their local organisation's policy. Where possible, mark all information with 'OFFICIAL' in the header and footer. Local organisational policy may override this requirement.

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.

Applying the OFFICIAL classification

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.

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.

OFFICIAL: Information whose compromise would typically cause limited to no negative consequences for policing, our partners (including damage to confidence in the confidentiality between policing and its partners) or to an individual.

Application of OFFICIAL-SENSITIVE caveat.

> *"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."* (GSCP, 2023)

Within the OFFICIAL tier, information or material whose compromise is likely to cause damage to the work or reputation of the organisation and/or policing 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.

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: Policing, HMG, the UK's international reputation, the UK economy, policing 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 Policing. Such information should be identified using the -SENSITIVE marking and additional handling controls apply. Use of this marking is recommended, but is at the organisation's discretion; users should consult their local organisation's policy.

In determining whether a -SENSITIVE marking and the related additional controls should be applied, forces should consider whether alternative risk management measures are proportional to the potential impact of the personal information being compromised.

Application of OFFICIAL-FOR PUBLIC RELEASE handling instruction.

> *"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."* (GSCP, 2023)

Where OFFICIAL information has been cleared for publication or is already in the public domain, the information creator/Information Asset Owner 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

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.

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/Information Asset Owner should consult with their Information Security Officer (or equivalent) to ensure the controls and/or behaviours are aligned with organisational policy and proportionate to the local risk appetite.

Additional Markings

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.

There are several different types of additional markings, including: the -SENSITIVE marking, handling instructions, descriptors, codewords, prefixes and national caveats. Your local organisational policy on should give further guidance as to how and when your force uses these markings.

To read more guidance on Additional Marking and how they may apply to your information please refer to the national Government Security Classification policy which can be found here: [Government Security Classifications Policy (HTML) - GOV.UK (www.gov.uk)]

OFFICIAL baseline behaviours table

OFFICIAL	OFFICIAL information 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 the force or policing. - 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/Information Asset Owner 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.

Verbal information

OFFICIAL	OFFICIAL information marked - SENSITIVE
Meetings & Discussions: - Only discuss using corporate devices or devices that have been approved by your organisation: – 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 all areas, including 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 appropriate.	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 – 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

OFFICIAL	OFFICIAL information marked - SENSITIVE
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: - 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.	**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 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.

Hard copy information - Transportation

OFFICIAL	OFFICIAL information marked - SENSITIVE
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.	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.

Hard copy information - Destruction

OFFICIAL	OFFICIAL information marked - SENSITIVE
- 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; that policy must include guidance on acceptable disposal e.g. using a cross-cutting shredder. 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.	- 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; that policy must include guidance on acceptable disposal e.g. using a cross-cutting shredder. Heads of Security in policing 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

OFFICIAL	OFFICIAL information marked - SENSITIVE
- 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.	- 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.

Electronic information - accessing

OFFICIAL	OFFICIAL information marked - SENSITIVE
- 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.	- 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 - Do not read in public. - Working remotely: do not access where you can be overlooked.

Sharing OFFICIAL information electronically (via corporate approved channels):	
OFFICIAL	**OFFICIAL information marked - SENSITIVE**
- 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.	- Information can be shared with individuals inside and 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.

Risk Management of information assets

When classifying assets, the creator and organisation should consider the risk and the controls which can be applied when handling information assets. Creators should review risk appetites of their organisation and NPCC guidance documents to apply appropriate controls. The risk appetite table, Annex A of National Police Information Security Risk Management Framework, should be used as a reference.

Reclassifying an information asset

Only the information creator from the originating organisation in consultation with the Information Asset Owner can reclassify and/or change the classification of an asset.

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).

Publication or Disclosure

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). Disclosure may also be required to Local Archives and/or museums under the NPCC Heritage Model (heritage-maturity-model.pdf at npcc.police.uk)

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.

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

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 Officer if compromised information contains personal data.

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:

- Accessing information from any device other than one accredited and/or approved by their organisation.
- Accessing SECRET or above information without authorisation.
- Viewing information or holding SECRET or above conversations outside of designated areas in line with issued organisational guidance.

All information users are expected to understand their organisation's breach policy and legal obligations, including under the Official Secrets Act (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.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed with information security officers (ISOs) and Information Management teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.
Measurables generated by adopting this standard can also form part of regular cyber management.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the guideline continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

ANNEX A – Working at SECRET

Working at SECRET

> ***"SECRET information is much more sensitive than OFFICIAL information. Due to the sensitive nature of SECRET information, the threat profile anticipates the need to defend against a higher level of threat actor capability than would be typical at the OFFICIAL level. A compromise of SECRET information has serious implications. It could: threaten the lives of individuals or groups; and/or seriously damage the UK's security resilience, international relations, financial security; and/or, impede the UK's ability to investigate serious and organised crime."*** (GSCP, 2023)

The SECRET classification tier is used for sensitive information that requires enhanced protective controls, the use of appropriately assured IT and heightened user discretion to guard against compromise.

Nonetheless, SECRET information still needs to be shared readily and promptly across HMG, the wider public sector and international and commercial partners; albeit using strict need-to-know principles. SECRET information is often time critical and needs to be operationalised - for example, 'action on' intelligence, counter-terrorism and organised crime or sensitive equipment procurements. Information creators should be mindful of not over-classifying information to TOP SECRET, which may restrict the ability to share it as readily and promptly across policing.

The sensitivity of SECRET information and the risks associated with its compromise need to be balanced against the risks of not sharing the information with colleagues who have a genuine need-to-know. Consequently, the associated baseline security behaviours and protective controls need to be agile and innovative, incentivising the right user behaviours, such as: exercising situational awareness; being accountable for security decisions and classifying correctly.

The information creator is responsible for assessing the potential impact of a compromise of information and the expected threat profile to determine whether information is SECRET. The serious impact of a compromise of information, combined with the enhanced risks expected from highly capable threat actors, is what defines SECRET classified information.

Applying the SECRET classification

Users working on SECRET information, whether in the office or at home (or in exceptional circumstances away from the office or home), should be briefed by their security teams on their responsibilities in the handling of SECRET information and equipment in a careful and secure manner.

Some information may only be classified as SECRET for a set (possibly short) period of time. The sensitivity of information can evolve through its life cycle e.g. information detailing a closely-held sensitive public announcement might be classified as SECRET until it is announced, but 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. Reclassifying material over its life cycle is important; it can avoid the proliferation of data assets requiring unnecessary security controls and resources, which is burdensome and expensive. It is also the responsibility of the information creator to inform previous recipients if classified information has been downgraded to OFFICIAL. In such circumstances, information creators should also consider whether additional markings apply to the downgraded information (such as - SENSITIVE).

Application of the SECRET baseline behaviours

At SECRET, information handling and security requirements must be clearly communicated to recipients, and all recipients must have a clear need-to-know.

The potentially serious impacts of a compromise of SECRET information, combined with the heightened threat profile, justifies enhanced (but proportionate) security behaviours and controls when compared to OFFICIAL. A set of baseline behaviours for users working at SECRET is outlined in the table below.

SECRET baseline behaviours table

Verbal information

Meetings & Discussions:

- Discuss only on IT or phone systems approved by your organisation's information security team for use at SECRET.
- The chair of the meeting must make it clear before the meeting begins that SECRET information will be discussed, ensure everyone present has the appropriate clearance, and should make clear any limitations or restrictions around further dissemination.
    - In public: Do not discuss.
    - In the office: Use meeting rooms so conversations cannot be overheard and use headphones (approved by your organisation) where possible.
    - If working remotely: Discuss using devices issued by your organisation for use at SECRET and use a private environment where conversations cannot be overheard by unauthorised personnel. Use headphones approved for use with the SECRET system.

    - Do not work on SECRET devices or work at SECRET in the presence of unauthorised personnel, or staff with the appropriate clearance but without a need-to-know.
- Do not discuss if there are any smart listening devices in the room (e.g. voice activated speakers), and remove all personal communication devices and wearable technology (such as a smart watch) from the room unless expressly risk assessed and permitted by an individual organisation or information system owner, or the device's vulnerabilities are mitigated with suitable personal communications devices audio countermeasures.
- Organisations should also consider carrying out periodic technical surveillance countermeasures (counter eavesdropping) sweeps of controlled office areas that frequently host SECRET meetings.
- Meeting attendees can brief back to their team members with the appropriate clearance based on the need-to-know principle, but they should check with the information creator if sharing further and should only brief staff in a suitably secure area for processing SECRET.

Hard copy information

Storage & Access

- In the office:
    - Store hardcopy information in National Protective Security Authority (NPSA) approved physical security equipment for SECRET.
    - Print on corporate systems or devices approved by your organisation for use at SECRET. You should consider printing SECRET documents on pink coloured paper in certain environments to make them easier to recognise (in conjunction with your organisation's accessibility and sustainability guidance).
    - Documents that are printed must bear a copy number on the top right corner of the first page (e.g. 1 of 3, 2 of 3, etc).
    - SECRET information must be registered in the Protected Document Registry book (or equivalent) if being kept for more than 5 days.
- Working remotely:
    - Do not remove hard copies of SECRET information from the workplace, except in exceptional circumstances for remote work. Where it is necessary to work on hard copy SECRET information at home or some other remote working site, senior management and Information Security Officer approval must always be obtained in advance, unless this has been delegated to other officials in line with local organisation policy.
    - Always log in the Protected Document Register book (or equivalent) that hardcopy SECRET information is being taken out of the building.
    - Hard copy SECRET information must be kept in your possession or stored securely at all times when working remotely.

- Store hardcopy information and devices in approved tamper evident containers in physical security equipment / furniture provided by your organisation. Containers should be placed in a discreet location and checked regularly for tampering.
- Mark all information with “SECRET” in the header and footer and number each page.
  - If the SECRET information is to be shared with an international partner the ‘UK’ prefix must be added at the front of the marking before it is provided.
- Mark any files or groups of documents with the highest classification marking.
- Wherever possible, handwritten notes containing SECRET information are to be avoided. If they need to be taken, they must be treated the same as any other SECRET document.

Transportation

- Where possible, print SECRET material securely at the destination rather than transporting hard copy material between policing or cleared contractor sites. If documents must be moved from the office:
  - Conduct a Threat and Vulnerability Risk Assessment to understand the risks and how to mitigate them.
  - Senior management and Information Security Officer approval must always be obtained in advance, unless this has been delegated to other officials in line with local organisation policy.
- Limit knowledge of planned movements to those with a need-to-know and the appropriate clearance.
- Check the document out in the Protected Document Registry book whenever transporting hardcopy SECRET documents.
- Moving physical assets by hand:
  - SC & NPPV3/MV clearance as a minimum is required for carrying assets by hand.
  - Never access or read the information in public.
  - Risk assess the need for two people to escort the assets.
  - Tether pages together and number each page.
  - Package documents in robust and opaque double envelopes or other suitable packaging. Use approved tamper-evident packaging, in line with organisational policy.
  - Mark SECRET on the inner envelope/packaging only - it must not appear on the outer envelope / packaging.
  - Add a return address on both the inner and outer envelope/packaging.
  - Place assets inside a discreet third bag, or other suitable security container (e.g. locked briefcase) if carrying by hand outside of a government building.
- Moving physical assets by courier service/postal service domestically (i.e. from and to a UK postal address):
  - Include a return address on both the inner and outer envelope/packaging.
  - Include a delivery receipt in the inner envelope/packaging.

    - Package documents in robust and opaque double envelopes or other suitable packaging. Use approved tamper-evident packaging, in line with organisational policy.
    - Mark SECRET on the inner envelope/packaging only - it must not appear on the outer envelope / packaging.
    - Seek approval from senior management and Information Security team before sending assets by commercial courier/post in the UK, unless this has been delegated to other officials in line with local organisational policy.
    - Use a commercial mail courier service with track and trace service or a government courier approved by your organisation, or contact the Information Security team for guidance.
- Moving physical assets overseas:
    - By default, physical SECRET assets should be sent to the local Embassy/Mission using the diplomatic bag or military courier. Alternatively staff can consider accessing the SECRET assets electronically using accredited IT systems at the local Embassy/Mission.
    - Moving assets by hand carriage should only be considered in urgent situations where there is a clear business case and if permitted by the organisation under their internal rules.
    - Seek approval from the information creator and the Information Security team before sending SECRET assets overseas, unless this has been delegated to other officials in line with local organisation policy.
    - Mark classification on the inner envelope/packaging. Do not mark the outer packaging with the classification level.
    - Package documents in robust and opaque double envelopes or other suitable packaging. Use approved tamper-evident packaging, in line with organisational policy.
    - SC & NPPV3/MV clearance as a minimum is required for carrying assets by hand.

Destruction

- Always dispose of information in the office in accordance with the NPSA Secure Destruction Standard with products from the Catalogue of Security Equipment (CSE).
- Record destruction of hardcopy SECRET in the Protected Document Registry book.

Electronic information

Storage & Access

- Do not access SECRET material in public or in the presence of unauthorised personnel.
    - In the office: Only work in areas authorised by your organisation for SECRET or above. Do not work at SECRET in areas where there is a significant footfall of external visitors to the organisation and/or staff members without appropriate clearance.
    - Working remotely: Do not work where unauthorised co-residents, visitors or passers-by can overlook the information.

- Only draft, store or share electronic information on IT systems approved by your organisation for use at SECRET or above. Never store SECRET information on the corporate IT system for OFFICIAL or on personal devices.
- When away from your device or terminal, even for a short time, ensure it is locked and remove any key or Crypto Ignition Key (CIK).
- Working Remotely:
    - Avoid taking SECRET laptops to locations other than your home or workplace.
    - Always be discreet when using or transporting SECRET accredited devices, especially in publicly accessible locations and even when using secure containers.
    - Do not leave SECRET accredited laptops and mobile devices unaccompanied in locations which can be accessed by unauthorised personnel e.g. cars, coffee shops, or hotel rooms. Remove any token or CIK and keep discreetly in your possession separately from the device. Mobile devices should either be in your possession or in a secure container at all times.
    - SECRET accredited devices must be secured in a secure container or furniture provided for this purpose by your organisation when not in use.
    - Do not access SECRET IT systems via public Wi-Fi.
- Mark all information with “SECRET” in the header and footer.
    - If the information is to be shared with an international partner the ‘UK’ prefix must be added at the front of the marking before it is provided.
- Do not use IT equipment if there are any smart listening devices in the room (e.g. voice activated speakers), and remove all personal communication devices and wearable technology (such as a smart watch) from the room unless expressly risk assessed and permitted by an individual organisation or information system owner, or the devices vulnerabilities are mitigated with suitable personal communications devices audio countermeasures.

Emails

- Do not send information outside the Secure Isolated Network (e.g. do not send via an OFFICIAL email account or via the open internet).
- Do not share with anyone within or outside your organisation without the need-to-know and the appropriate clearance.
- Use clear handling instructions in the subject line and body of the email where appropriate.

Destruction

- Dispose of digital information in the office in accordance with the NPSA Secure Destruction Standard with products from the CSE and the NCSC’s ‘Secure Sanitisation of Storage Media’ guidance.

ANNEX B – Working at TOP SECRET

Working at TOP SECRET

> ***"A compromise of TOP SECRET information could cause exceptionally grave damage. It could cause widespread loss of life or threaten the security or economic wellbeing of the UK or friendly nations. The expected capability level of hostile threat actors is extremely high at this tier."*** (GSCP, 2023)

The TOP SECRET classification tier is reserved for the most sensitive information assets that directly support or inform the national security of the UK or its allies AND require extremely high assurance of protection from the most serious threats, with the use of Secure Isolated Networks and highly secure physical infrastructure.

The information creator must assess the potential impact of a compromise of information and the expected threat profile to determine whether information is TOP SECRET. The exceptionally grave damage of a compromise of information, combined with the enhanced capabilities expected from the most capable and well-resourced threat actors, is what defines TOP SECRET classified information.

Application of the TOP SECRET classification

The information creator is responsible for marking TOP SECRET information, which must only be used for the most sensitive assets. Before users can access TOP SECRET material for the first time, they must be briefed by their organisation's security team on how to handle the information and any related equipment in a careful and secure manner. It is the responsibility of organisations' security teams to ensure their users have routine refresher training thereafter. There is additional physical, personnel and technical guidance available for the TOP SECRET tier held at a higher classification. This is available from the Government Security Group; users should contact their security team for more information. The NCSC should be consulted where there is a business need for further guidance.

Application of the TOP SECRET baseline behaviours

TOP SECRET information justifies the most stringent behavioural, procedural and technical controls to protect against the highest capability of threat actors and to reduce the risk of an intentional or unintentional compromise. A set of security behaviours for users working at TOP SECRET is outlined in the table below.

At TOP SECRET, information handling and security requirements must be clearly communicated to recipients, and all recipients must have a strict need-to-know.

If additional security controls are necessary at a local level to manage specific risks, the information creator should consult with their Information Security team or equivalent to ensure the controls are aligned with organisational policy and proportionate.

Baseline behaviours and measures table:

Verbal information

Meetings & Discussions:

- The chair must make it clear before the meeting starts that TOP SECRET information will be discussed; assure that all attendees have the appropriate clearance; and, make clear any limitations or restrictions around further dissemination.
- Discuss only on IT or telephone systems approved by your organisation for use at TOP SECRET.
- In the office:
    - Use TOP SECRET accredited meeting rooms so conversations cannot be overheard. TOP SECRET environments can be assured against audio leakage and suitability to hold conversations. Contact UK NACE for guidance.
    - Use headphones (approved by your organisation) where possible.
    - Personal or corporate communication devices, wearable technology (such as smart watches) and smart listening devices (e.g. voice activated speakers) are prohibited from TOP SECRET areas, unless specifically approved by your organisation.
    - Meeting attendees can brief back to their team members with the appropriate clearance based on the need-to-know principle, but should check with the information creator if sharing further and should only brief staff in a suitably secure area for processing TOP SECRET. Where the information is not for further dissemination (even within teams) the chair should make this clear at the start of the discussion.
    - Technical surveillance counter-measures (counter eavesdropping) sweeps should be undertaken periodically to ensure the integrity of the meeting space.
- Items entering a TOP SECRET area such as furniture should be sourced appropriately and, if necessary, inspected for sign of tamper.
- In public:
    - Do not discuss.

Hard copy information

Storage & Access

- In the office:
    - Do not leave TOP SECRET material unattended.
    - Store hardcopy information in NPSA approved physical security equipment approved for TOP SECRET when not in use.

- Print on corporate systems or devices approved by your organisation for use at TOP SECRET. You should consider printing TOP SECRET documents on yellow paper to make documents easier to recognise (in conjunction with your organisation's accessibility and sustainability guidance).
- Documents that are printed must be tethered together and bear a copy number on the top right corner of the first page (e.g. 1 of 3, 2 of 3, etc).
- Register information in the Protected Document Registry book (or equivalent), noting the reference number on each TOP SECRET document.

- At home:
  - Remote working from home at TOP SECRET is not permitted.
- Mark all information with "TOP SECRET" in the header and footer.
  - If TOP SECRET information is to be shared with an international partner, the 'UK' prefix must be added at the front of the marking before it is provided.
- Mark any files or groups of documents with the highest classification marking of the document pack.
- Handwritten notes containing TOP SECRET information should be avoided. If they need to be taken, they must be treated the same as any other TOP SECRET document.

Transportation

- Do not take TOP SECRET information home under any circumstances.
- Where possible, print TOP SECRET material securely at the destination rather than transporting hard copy material between HMG or cleared contractor sites.
- If documents must be moved from the office:
  - Conduct a Threat and Vulnerability Risk Assessment to understand risks relating to moving the documents and how to mitigate these risks;
  - A clear rationale must be set out in writing; and
  - Senior management and Information Security Officer approval is needed, unless this has been delegated to other officials in line with local organisation policy.
- Strictly limit knowledge of planned movements to those with a need-to-know and the appropriate clearance.
- Check the document out in the Protected Document Registry book whenever transporting TOP SECRET documents.
- Moving physical assets by hand in the UK:
  - DV clearance as a minimum is required for carrying assets by hand.
  - Never access or read the information in public.
  - Two people (both cleared to DV) must escort the assets (unless within a specified Government Secure Zone).

- Package documents in robust and opaque double envelopes or other suitable packaging. Only use tamper-evident packaging approved by NPSA in the Catalogue of Security Equipment (CSE).
- Mark TOP SECRET on the inner envelope/packaging only - it must not appear on the outer envelope / packaging.
- Add a return address and user contact details on both the inner and outer envelope/packaging in case the package is lost or misplaced.
- Include a delivery receipt in the inner envelope/packaging. This delivery receipt must be returned immediately by the recipient.
- If carrying by hand outside of a government building, place assets inside a discreet, opaque and locked security container.

- Moving physical assets by commercial courier service/postal service domestically (i.e. from and to a UK postal address) is not permitted. An SA/SSA approved secure mail delivery service that has two DV cleared escorts should always be used.
- Moving physical assets overseas:
  - Seek approval from the information creator, the Senior management and Information Security team before sending assets by post overseas, unless this has been delegated to other officials in your organisation's local policy.
  - Package documents in robust and opaque double envelopes or other suitable packaging. Only use tamper-evident packaging approved by NPSA in the CSE.
  - Mark TOP SECRET on the inner envelope/packaging, do not mark the outer packaging.
  - Include a delivery receipt in the inner envelope/packaging. This delivery receipt must be returned immediately by the recipient.
  - Use an approved government courier service e.g. diplomatic bag or military courier (defence courier service).

Destruction

- Do not destroy assets without written approval from the information creator. Assets must be returned to the information creator in the first instance (unless written approval is given to the recipient to destroy the information in line with organisational policy).
- Dispose of information in the office in accordance with the NPSA Secure Destruction Standard. Use products from the CSE. Use an approved shredder.
- Destroy with a witness present (who also must be DV cleared). The person destroying the document and the witness must record the destruction in the Protected Document Registry book.

Electronic information

Storage & Access

- Only work in areas authorised by your organisation for processing TOP SECRET in the office using approved equipment.

- Never access or read TOP SECRET material in public or in the presence of unauthorised personnel.
- Mark all information with "TOP SECRET" in the header and footer, and number each page.
    - If the information is to be shared with an international partner the 'UK' prefix must be added at the front of the marking before it is provided.
- Only draft, store or share electronic information on IT systems approved by your organisation for use at TOP SECRET. It is prohibited to store TOP SECRET information on any system or device not specifically approved for TOP SECRET. This includes the corporate IT system for OFFICIAL or SECRET and personal devices.
- Lock devices when leaving your workspace for any length of time, even briefly.

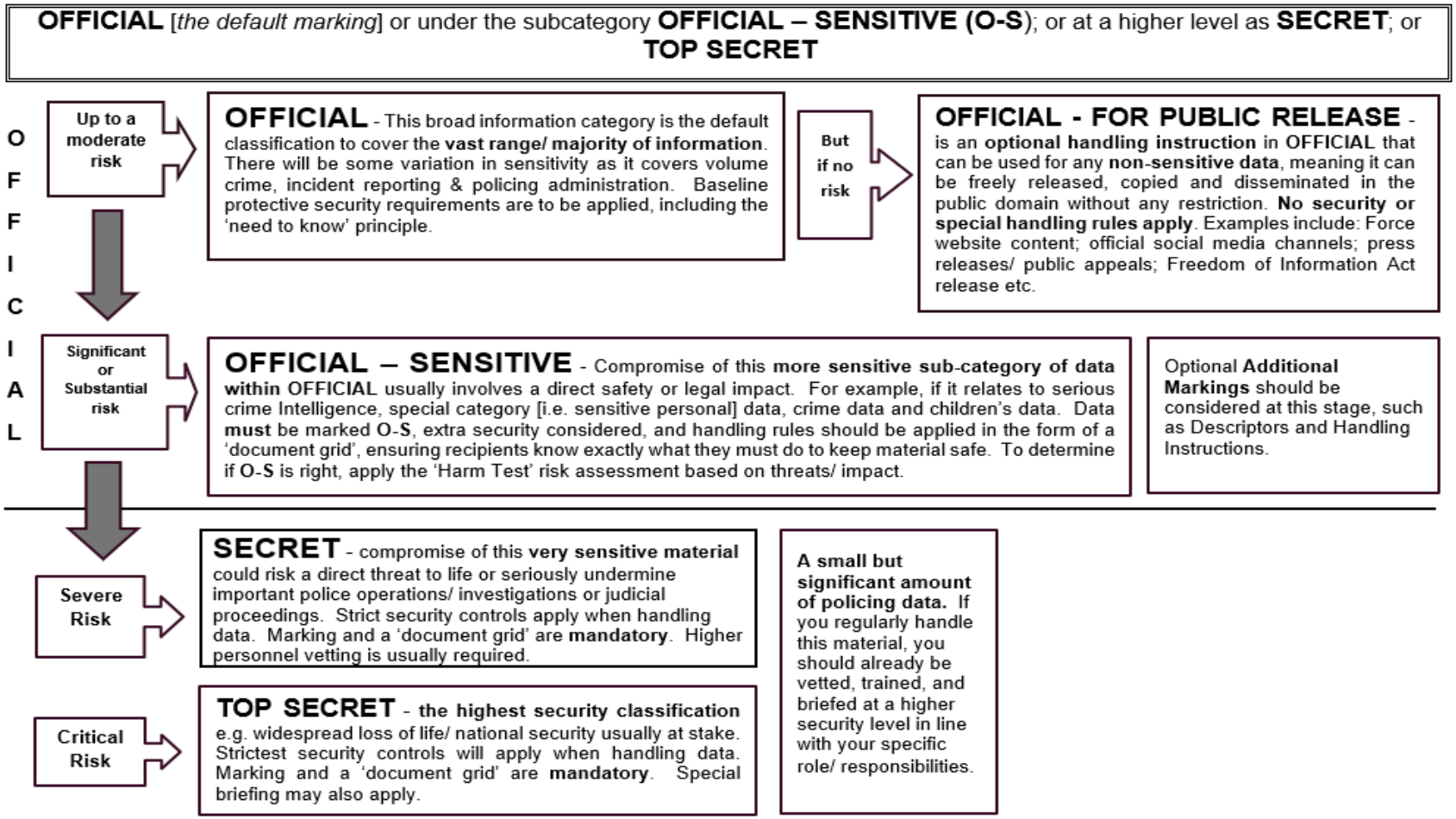
Emails

- Do not send information outside the Secure Isolated Network.
- Do not share with anyone outside your organisation without authorisation from the information creator and without need-to-know.
- Use clear handling instructions in the subject line and body of the email where appropriate.

Destruction

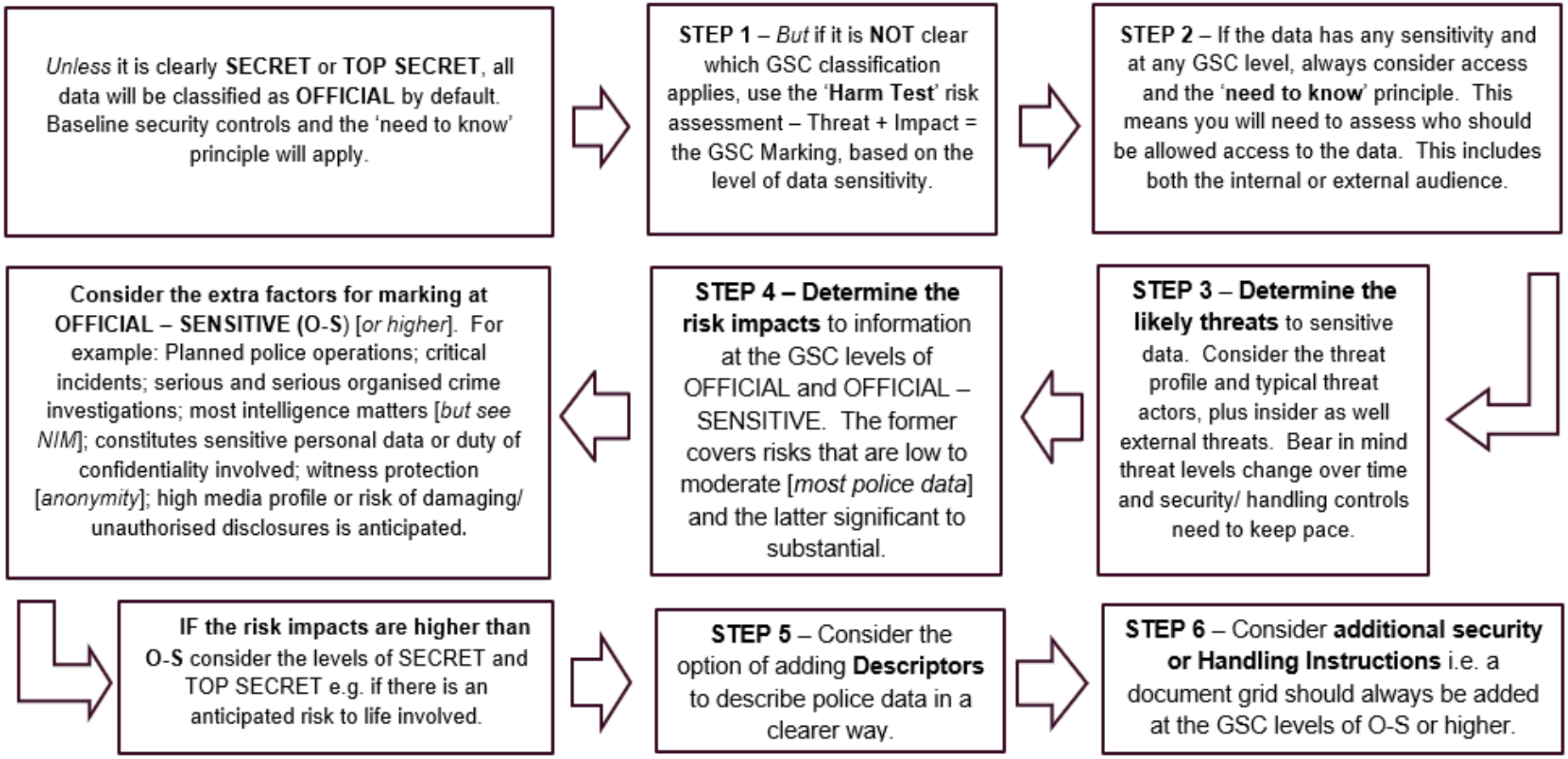
- Dispose of digital information in the office in accordance with the NPSA Secure Destruction Standard and using products from the CSE. Also see the NCSC's 'Secure Sanitisation of Storage Media' guidance.

ANNEX C – Classification guidance quick reader guide



1.(a) OFFICIAL [*routine police business with usually some sensitivity attached; so risk assess if moving data outside trusted police environment*] - **RISK LEVEL = LOW to MODERATE**	**1. (b) OFFICIAL – SENSITIVE** [*"**SENSITIVE**" – a sub-category within **OFFICIAL**]. Due to higher sensitivity extra security controls/ handling rules **must** be communicated to others when moving outside of a secure area*] **RISK LEVEL = SIGNIFICANT to SUBSTANTIAL**
Majority of Police information is OFFICIAL – operational and admin/ support data. It is to be freely shared with other forces and usually with key trusted partners [e.g. Criminal Justice community, social services, service providers, etc.]. May require secure transfer method so risk assess sensitivity. Examples: • Routine [volume] crime [Magistrates Court]/ incident reports/ prosecutions/ custody procedures/ general victim/ witness care; • Community policing/ general enquiries/ emergency response and call handling; • BAU provision/ management of police admin/ licensing/ support services e.g. HR/ Finance/ Estates/ ICT/ Equipment [vehicles/ uniform/ radios]. • **Suitable for Publication** – This classification is as an optional descriptor for any non-sensitive data. This allows material to be re-used freely, including publication in the public domain or transmission to partners.	**Only transfer/ share O-S outside police service on a legal basis** [DSA/ statutory disclosure etc.]. Examples: • Serious/ organised crime reports/ prosecutions [Crown Court, including sentencing]; • Significant safety risk/ public protection of children/ vulnerable adults/ vulnerable witnesses; • Planned policing/ security operations/ events; • Usually lowest security level for intelligence - but use the National Intelligence Manual [NIM] handling codes to inform GSC needs; • Protecting personal data/ special category [i.e. sensitive personal] data, crime data or children's data to avoid a breach of the Data Protection Act [DPA] 1998/ UK GDPR; • Confidentiality of sensitive or commercial negotiations; and • Handling security incidents/ significant impacts on police
2. SECRET *[Major step up from O-S regarding security needs].* **RISK LEVEL = SEVERE**	**3. TOP SECRET** [R*elates to highest degree of sensitivity justifying strictest security controls*] **RISK LEVEL = CRITICAL**
SECRET covers **a small but exceptionally significant amount of policing data** that is received, created and processed. Examples are: • Protecting individuals against **loss of life**; • Handling most serious organised crime; dangerous offender management; witness protection and responding to the threat of terrorist attack; • Dealing with major events/ serious public disorder that would affect the police service/ HMG services or UK essential infrastructure. • Loss of data would have a major impact on intelligence/ operational capabilities for at least a month; cause a major/ key court case to collapse or have a major impact on police finances [£millions]. • Intelligence on most serious cross-border organised crime/ specialist crime investigations/ international events/ major risk to integrity of the judicial system; • Covert surveillance/ Investigatory Powers Act 2016/ Covert Human Intelligence Source [CHIS] management; • May also lead to loss of trust in police [by public/ HMG], impacting on intelligence and operational capabilities.	This is the **highest possible UK Government security classification**, demanding the highest level of protection from multiple cyber, physical and other threats. Most personnel **will not** regularly handle such material unless they are in a specific role with the highest level of security clearance. **Strict security controls/ environment are always enforced**. Examples include: • Where there is a real/ credible and the gravest/ critical threats leading to a high risk of **mass loss of life**/ close security - high risk targets/ VIPs/ witness protection etc.; • All Security Service/ counter-terrorist intelligence/ communications with police service; and • The close protection plans for important persons/ ensuring security of national government/ democratic institutions/ Critical National Infrastructure etc.

Process for GSC risk assessment of information (data)



Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Ben Walker	Initial Version	09/11/23
0.2	Ben Walker	Internal peer review	27/11/23
0.3	Ben Walker	Post NCPSWG review	09/01/24
0.4	Ben Walker	Additional police context added	04/03/24
1.0	Ben Walker	Included amendments requested at NCPSWG and migrated to 2024 template.	23/04/24

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	17/04/24

Document References

Document Name	Version	Date
NIST Cyber Security Framework	v1.1	04/2018
National Police Information Security Risk Management Framework v1.0.pdf	V1.0	05/2023
Secure Destruction | NPSA	Web Page	Accessed 23/04/24
Government Security Classifications - GOV.UK (www.gov.uk)	Web Page	Cabinet Office 30/06/23
The Catalogue of Security Equipment | NPSA	Web Page	Accessed 23/04/24
Secure sanitisation of storage media - NCSC.GOV.UK	Web Page	Accessed 23/04/24