Data Handling Policy for Supply Chains

Purpose:

1. This Policy provides an overview of the way you must manage and handle information that is owned or required by Highways England to ensure its security. It describes the protective markings you must use, and explains what you must do when communicating information to us through e-mail or by using removable media.

Introduction:

2. Different types of information must be handled in different ways. It is the content of the information that determines how it is stored and handled, and what protection it should be given. You must always consider the content of the information, before making a judgement on what level of protection to apply.

3. All electronic documents and records must be saved into an Electronic Document and Records Management (EDRM) System or other storage facility approved by our Company Records Officer. Any draft information must be clearly marked as DRAFT.

4. Physical records that either must not be stored electronically (see below), or are required to be kept as a physical, paper copy, must be kept within an official, registered paper filing system.

5. It is a good overall rule that you should treat Highways England information, especially if it is officially protectively marked, as if it were a large amount of your own cash.

Levels of protection and Protective Markings

6. There are three security classifications described in the Government Security Classification Policy, OFFICIAL; SECRET and TOP SECRET. It is anticipated that virtually all our information will sit in the OFFICIAL classification.

7. It is the sensitivity of the information that decides how you should classify, handle, store and transmit it.

Application of Protective Markings

8. Information assessed as OFFICIAL does not require marking. Any information that is assessed as being of a significantly sensitive nature should be marked OFFICIAL-SENSITIVE. A caveat may be applied to determine the kind of sensitivity, so for example OFFICIAL-SENSITIVE PERSONAL or OFFICIAL-SENSITIVE COMMERCIAL. These classifications must be clearly visible on the document itself, either as a watermark, or in the heading or clearly included in a footnote, so that if it is printed off the marking can still be seen on the hard copy. The marking should also be clearly marked on the description of documents

either as part of the file name, if electronic or on the cover of the folder for paper documents.

9. The policy anticipates the use of OFFICIAL-SENSITIVE as a classification will be limited to a very small amount of information that requires a higher level of handling protection than most of what we handle every day.

Levels of Protection and Security Classification

Classification	Examples
OFFICIAL	The majority of information that is created or processed by the public sector falls into this category. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile. No marking need be physically applied. • Day to day business of government, service delivery and public finances • Public safety, criminal justice and enforcement activities • Commercial interests, including information provided in confidence and intellectual property • Routine international and diplomatic activities • Many aspects of defence, security and resilience • Personal information that requires protection under the Data Protection Act (1998) or other legislation (e.g. health records)
OFFICIAL-SENSITIVE	If you deem the information to have sufficient sensitivity that it requires additional handling controls to be put in place to give additional protection, mark it OFFICIAL-SENSITIVE. • Sensitive corporate or operational information e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues. • Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court proceedings • Sensitive personal data e.g. health records, financial details, that it is not considered necessary to manage in the SECRET tier • Policy development and advice to ministers on contentious and very sensitive issues • More sensitive information about defence or security assets or equipment • Commercial or market sensitive information, including that subject to statutory or regulatory

	obligations, that may be damaging to HMG or to a commercial partner if improperly accessed
SECRET	It is unlikely that we will produce information in this classification, although there may be occasion when it may have to handle it from external agencies. In these circumstances please contact the IT security advice team. Information with a SECRET classification is comprised of very sensitive information that justifies heightened protective measures to be deployed to defend against a determined and highly capable threat actor, e.g. where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.
TOP SECRET	It is highly unlikely that we will either produce or have access to information in this category. In these circumstances please contact the IT security advice team. Information in the TOP SECRET classification is the HMG's most sensitive information, requiring the highest levels of protection against the most serious threats, e.g. where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

10. The table below gives a summary of the correct storage locations for the different levels of protection.

Level of Protection	Correct Storage Location	
	Electronic	Physical
OFFICIAL	EDRM or approved filing system (Good commercial practice, broadly ISO 27001 compliant with details provided to us)	Registered paper file.
OFFICIAL-SENSITIVE	EDRM or approved filing system (Good commercial practice, broadly ISO 27001 compliant with details provided to us)	Registered paper file with appropriate marking
SECRET and TOP SECRET	You must consult our IT Security Team	You must consult our IT Security Team

- **CONFIDENTIAL must not be confused with "Commercial in Confidence".**

Sending Documents by E-Mail.

11. The following table gives some guidance on what information you are able to transmit by e-mail. However, the nature of the Government Security Classification policy provides for far greater emphasis on using your own judgement and expertise to protect the information that you work with. The baseline judgement is the need-to-know principle and ensuring appropriate handling instructions accompany the information.

	OFFICIAL	OFFICIAL-SENSITIVE	SECRET/TOP SECRET
Can I e-mail the information to a PSN* address?	Yes	Yes	No
Can I e-mail information outside the PSN?	Yes	Possibly	No
Can I e-mail the information to my home e-mail?	No	No	No
Can I e-mail the information to a colleague's home e-mail?	No	No	No
Can I e-mail the information to my boss's home e-mail if s/he tells me to do so?	No	No	No

*PSN: Public Sector Network. This includes both GSI and pnn.police.uk mail addresses

12. When sending OFFICIAL-SENSITIVE information, the marking must be included in the Subject line of the e-mail and the first line of the text body, along with any specific handling instructions, eg “Not for release until…” .

The Use of Removable Media

Using removable media

13. “Removable media” is a generic term for media used to physically carry electronic information. Examples include:

- CD-ROMs and DVDs
- IronKey USB memory sticks
- DiskGenie Portable hard drives
- Digital cameras and mobile phones

14. If the information to be stored on the removable media is part of a data set for which an Information Asset Owner has been appointed, then you will need to obtain the approval of the Information Asset Owner.

15. Removable media should not be used as a permanent storage medium for information unless such use is part of an official, fully documented and approved process. In most cases, the appropriate storage location for electronic information will be in an EDRM, as detailed at paragraph 10 above.

16. Any removable media containing Highways England information must be looked after as securely as the equivalent paper documents. As a benchmark, if the information is OFFICIAL SENSITIVE, you must treat it as if it were the equivalent of a large amount of your own cash.

17. If you use a safe or other secure container for the short-term storage of removable media, you must make sure it is fire-rated for removable media. At temperatures where paper would still be safe, tapes, CDs and DVDs will have melted and other removable media such as USB sticks will have been permanently damaged.

18. On every occasion that removable media is brought into or received by an office, it must be virus-checked before being attached to any part of your IT network.

19. Floppy disks of any sort may no longer be used for storing any Highways England information. In the unlikely event that you are holding official information on this kind of media, please arrange to transfer it to the appropriate storage system (most likely your EDRM) and to dispose of the floppy disks.

Use of Third Party Removable Media

20. Only encrypted hard drives or USB memory sticks issued by Highways England may be used for transferring protectively marked information as they will be connected to our ICT equipment at some point. The use of USB memory sticks belonging to any business partner or any other third party is not permitted.

21. CDs and DVDs belonging to our supply chain may be used to transfer information to Highways England systems. Such media is subject to all the restrictions as set out in this document, and can only be used to transfer information that is not protectively marked. They must also only be used with the knowledge of the appropriate Highways England team leader or senior manager. Information must not be written from Highways England systems to removable media not belonging to Highways England.

Use of Personal Removable Media

22. You must not use personally-owned removable media for storing government information, or connect it to any part of our IT network (even if only to recharge it).

23. Any removable media owned by a third party found connected to our IT network may be removed for examination by our Security Team. The owner will be reported to their company, and the media may become Highways England property. In such cases, we are not obliged to offer any form of compensation for the media.

Protectively marked Information and Removable Media

24. The following table sets out clearly what information you are allowed to place on removable media. These protection measures depend on the following factors:

- the protection level being applied to the information;
- The type of removable media, and whether or not it is encrypted
- The ownership of the removable media

	Protective marking		
	OFFICIAL	OFFICIAL SENSITIVE	SECRET / TOP SECRET
Can I receive information on CDs/DVDs or portable hard drives belonging to our supply chain or another third party?	Yes	Possibly	No
Can I place information on CDs/ DVDs, memory sticks or portable hard drives belonging to our supply chain or another third party?	No	No	No
Can I place information on CDs or DVDs issued by HE or Government department?	Yes	Possibly	No
Can I place information on encrypted memory sticks or hard drives issued by HE or Government department?	Yes	Yes	No
Can I place information on an official, encrypted laptop?	Yes	Yes	No
Can I place information on my own removable media, smartphone, tablet, laptop, PC, etc.?	No	No	No

25. Where OFFICIAL-SENSITIVE information is placed on removable media, it must be clearly labelled OFFICIAL-SENSITIVE.

Re-using Removable Media

26. Before re-using encrypted memory sticks or hard drives, they must be fully re-formatted. It is good practice to delete files from these after they are no longer needed.

27. Encrypted memory sticks or hard drives must not be passed on to other organisations or individuals for re-use. They must be returned to Highways England.

28. Remember that deleting information from media does not remove the information on it. It only removes the “markers” on the media that point to where the information really is. This allows the space on the media to be re-used. It is possible to “undelete” such information, even if it has been partly over-written.

Disposing of Unwanted or Unusable Media

29. All media which carries or has carried protectively marked or other sensitive information must be disposed of according to HMG guidelines. Please contact our IT security team for details before disposing of it.

Reporting loss or theft of information

30. Loss or theft of any government information must be reported to the IT Security Team as soon as possible.

Exceptions to these Requirements

31. In exceptional circumstances, it is possible to apply to our Senior Information Risk Owner (SIRO) for agreement to depart from the requirements set down in this policy.

32. If you wish to seek an exception, you must approach your Highways England contact, who will work with our IT Security Officer to decide if an exemption is warranted.

33. For further information on this Policy, please consult either our Company Records Officer or our IT Security Team via **ITSecurityAdvice@highwaysengland.co.uk**

Information Strategy Policy & Assurance
Information & Technology Directorate