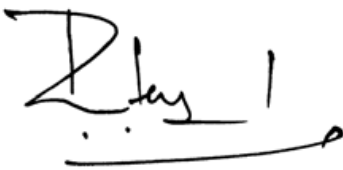




# Protective Marking Policy

## A.7.2.2



Signed .....

Date: 25 September 2009

Peter Neyroud, CEO NPIA

© - [National Policing Improvement Agency](#)

For copyright specific enquiries, please telephone the NPIA National Police Library on 01256 602650.

**TABLE OF CONTENTS**

Identification ..... 4

ISO/IEC 27001:2005 ..... 4

Ownership..... 4

Revision History ..... 4

Approvals..... 5

Distribution ..... 5

Equality Impact Assessment ..... 5

Legal Validation ..... 5

Process Map ..... 5

1. INTRODUCTION ..... 6

2. POLICY AIMS ..... 7

3. POLICY DETAIL ..... 7

    3.1 Principle ..... 7

    3.2 Definitions ..... 7

        3.2.1 What is Protective Marking?..... 7

        3.2.2 What is an asset?..... 8

        3.2.3 What is asset confidentiality? ..... 8

        3.2.4 What is asset integrity and availability?..... 8

        3.2.5 What are the threats to our assets? ..... 8

    3.3 Classifications..... 9

        3.3.1 Descriptors..... 9

        3.3.2 Special handling instructions..... 9

        3.3.3 'Time Sensitive' Assets..... 10

    3.4 Creation and Marking of Information Assets..... 10

        3.4.1 Criteria ..... 10

        3.4.2 Process for assessing the Protective Marking..... 12

        3.4.3 Layout and Labelling..... 14

        3.4.4 Protective Marking Responsibility..... 15

        3.4.5 Change Process ..... 15

3.5	Handling and Transfer .....	15
3.6	Storage .....	16
3.6.1	Electronic data.....	16
3.6.2	Physical assets .....	16
3.7	Disposal .....	16
4.	IMPLICATIONS OF THE POLICY .....	17
4.1	Training Requirements.....	17
4.2	IT Infrastructure .....	17
4.3	Related Policies.....	17
5.	MONITORING AND REVIEW .....	17
	ANNEX A - Impact Level Definition Tables .....	18
	▪ Table 1 - Defence, Intn'l Relations, Security and Intelligence.....	18
	▪ Table 2 – Public Order, Safety and Law Enforcement .....	19
	▪ Table 3 – Trade, Economics and Public Finances .....	20
	▪ Table 4 – Public Services: impacts, disruption, compromise, etc .....	21
	▪ Table 5 – Critical National Infrastructure (CNI) .....	24
	ANNEX B - Protective Marking Table.....	26
	ANNEX C - Table of Descriptors .....	27
	ANNEX D - Summary of Handling, Transfer & Disposal Requirements.....	28
	ANNEX E – Minimum Scope of Protected Personal Data .....	30

### Identification

Policy Title: Protective Marking Policy  
Version: 1.2  
Policy Reference Number: NPIA042  
Document Location: Stored on the policy database and accessible via the Intranet

### ISO/IEC 27001:2005

Reference: A.7.2.2  
Policy Level: Tier 3  
Superordinate Policy: A.7 – Asset Management Policy

### Ownership

Directorate Responsible: Information and Communications Technology and Science (ICTS)  
Department Responsible: Chief Technology Officer Unit  
Policy Owner: Senior Information Risk Manager (Adam Clark)

### Revision History

Effective From: 25 Sep 2009  
Next Review Date: 23 July 2010

<b>Revision Date</b>	<b>Previous Revision Date</b>	<b>Summary of Changes</b>
25/09/09	31/07/08	V1.2 – changed policy ownership details, and the review date put back by 1 year due to restructure within the organisation.
31/07/08	23/07/08	V1.1 – information added to the table in Annex D.

**Approvals**

This document requires the following approvals:

Name	Title	Date of Approval	Version
Peter Neyroud	CEO	23/07/08	1.0
Information Assurance Governance Board		02/07/08	1.0

**Distribution**

This document has been distributed to:

Name	Title	Date of Issue	Version
All Staff		25/09/09	1.2
All Staff		31/07/08	1.1
All Staff		24/07/08	1.0

**Equality Impact Assessment**

Has an EIA been completed?

Yes No

If no, please indicate the date by which it will be completed.

If yes, please send a copy of the EIA with the policy.

**Legal Validation**

Has the policy been legally validated?

Yes No

**Process Map**

Has a process map been completed?

\*N/A Yes No

(\* Not Applicable)

## **1. INTRODUCTION**

This policy applies to all categories of NPIA employees including (whether full-time or part-time) all employees (fixed term and permanent) and seconded staff. It also applies to temporary and agency staff, self-employed consultants, contractors and to associate tutors. In addition, where customers, students, visitors or any other individual is working at, residing or visiting the NPIA's property or using the NPIA's assets, responsibility rests with their hosting/employing business unit to ensure that they are aware of and comply with all relevant sections of this policy. Hereinafter, each of the above named parties will be referred to as employees for the purposes of this policy.

The Senior Information Risk Manager owns this policy and can be contacted for any queries regarding the policy content, by email to:

[information.assurance@npia.pnn.police.uk](mailto:information.assurance@npia.pnn.police.uk)

Consultation has taken place with the Information Assurance Tactical Group, the Information Assurance Governance Board, the Equality Diversity and Human Rights Unit, the Legal Services Unit and the Secretariat policy team.

The NPIA often holds data that has certain sensitivities, eg, employee bank account details, details of current Criminal Cases even the details of its safe combinations – in other words, data that we would not want to be shared with everyone. This data must be protected to ensure that it is only seen by those individuals who need to see it as part of their role within the NPIA – this is referred to as “Need to Know”.

The NPIA must also store each piece of information in an appropriately secure manner, eg, individuals would not want to have to have to open a locked door to collect every document they printed, but they would probably want to if the document contained their personal details!

To deal with these issues the Government has created a common way of valuing information which allows a set of rules and procedures to be set for the creation, storage, transfer and destruction of information in whatever form it takes, based on the value that it is given. This system is known as the **Government Protective Marking Scheme (GPMS)** and is a mandatory requirement for all Government Departments, Non Departmental Public Bodies (NDPB's) and UK Police Forces. The common use of the GPMS facilitates sharing of information between Government, Police Forces and other Criminal Justice organisations, by ensuring that information will be treated the same way no matter who has it.

## **2. POLICY AIMS**

- To inform employees of the Protective Marking standards and protocols that must be followed.
- To provide consistent and clear methodology on the Marking of information assets.
- To ensure that the NPIA is compliant with Government information security standards required to maintain accreditation to the Criminal Justice eXtranet (CJX) which is an essential part of the NPIA's business.

## **3. POLICY DETAIL**

### **3.1 Principle**

It is the policy of the NPIA that the requirements mandated within the GPMS will be fully applied to all information assets created, managed, handled, stored or otherwise processed within the NPIA.

### **3.2 Definitions**

#### **3.2.1 What is Protective Marking?**

Protective Marking is all about protecting the confidentiality, integrity and availability of NPIA's business assets from a wide range of threats.

### **3.2.2 What is an asset?**

The term 'asset' can be applied to anything that is of value to and necessary for the success of NPIA business (eg, employees, with their knowledge, skills and experience; information systems; data; equipment; money; property; vehicles etc can all be valuable business assets).

### **3.2.3 What is asset confidentiality?**

When we consider security, the first thing that we usually think about is 'keeping secrets secret'. In Protective Marking terms this is known as asset 'confidentiality'. In practice, maintaining asset confidentiality means limiting access to, and often knowledge of, sensitive information and other assets to individuals who 'need to know' about them to effectively carry out their work.

### **3.2.4 What is asset integrity and availability?**

To be fully effective in your work, the NPIA will need to provide you with timely access to appropriate, complete, accurate and reliable assets: essentially, this is what asset 'integrity' and 'availability' is about. In many instances protecting the integrity and availability of assets may be a higher priority than that of asset confidentiality. Eg, it is probably more important for budget holders to be able to access their spend to date figure when they want (Availability) and know it is correct and has not been tampered with (Integrity) than it is for the figure to be kept from other people.

### **3.2.5 What are the threats to our assets?**

Criminals, foreign intelligence services, investigative journalists, pressure groups and protesters, terrorists, hackers and computer viruses, natural disasters such as floods and sadly, disgruntled or dishonest employees are all known threats to our assets.

### **3.3 Classifications**

There are 4 classifications of Protective Marking that you can apply to sensitive assets and one sub-marking level, depending on the degree of sensitivity involved:

- RESTRICTED (and the sub-national marking PROTECT)
- CONFIDENTIAL
- SECRET
- TOP SECRET

When you apply a Protective Marking to a sensitive asset you are in effect indicating its value in terms of the damage that is likely to result from its compromise. To help prevent this happening, the Protective Marking you use indicates the type of security controls needed to protect the asset and determines the level of security clearance needed by those who will be given access to it. In reality, the vast majority of sensitive assets will only need to be marked PROTECT, RESTRICTED or CONFIDENTIAL.

#### **3.3.1 Descriptors**

In addition to the protective marking itself, 'DESCRIPTORS' may be added, but only in cases where it adds meaning to the protective marking, as overuse will devalue their impact. Examples are RESTRICTED – STAFF or RESTRICTED – COMMERCIAL. The exception to this is where the sub-marking PROTECT is used, which always requires the addition of a Descriptor. Please refer to the Table of Descriptors in [Annex C](#).

#### **3.3.2 Special handling instructions**

Depending on the type and nature of the asset, in addition to a Protective Marking you may also wish to consider applying special handling instructions. These can be applied in the form of DESCRIPTORS, CAVEATS, NICKNAMES and CODEWORDS or, exceptionally, other handling instructions.

When you use a special handling instruction you are simply further limiting the circulation of and access to the Protectively Marked asset within addressee organisations (eg, an asset marked RESTRICTED CONTRACT, means that in addition to the security controls indicated by the Protective Marking, the (CONTRACT) descriptor would indicate that only those directly involved with the contract should be given access to it).

### **3.3.3 'Time Sensitive' Assets**

In certain circumstances you may wish to apply a Protective Marking which is 'time sensitive'. That is, at the time of origination the sensitivity of an asset may merit the application of a Protective Marking. But, at some time in the relatively near future the sensitivity will no longer apply and therefore the Protective Marking effectively ceases to be needed or may be downgraded (e.g. Budgetary papers may be marked CONFIDENTIAL BUDGET prior to discussion in Parliament, after which the subject matter is in the public domain and is no longer sensitive so the marking is not needed).

## **3.4 Creation and Marking of Information Assets**

### **3.4.1 Criteria**

It is important to emphasise that the majority of NPIA information systems are only Accredited for the processing of information assets that are marked up to and including RESTRICTED. Only a very few NPIA information systems are Accredited at CONFIDENTIAL or above.

Where an information asset needs to be created which appears to require marking at a higher level than the information system is Accredited to, advice must be sought from the NPIA Security & Business Continuity Unit. It is anticipated that circumstances leading to a need to create such material in day-to-day NPIA business will be very rare.

Special arrangements are already in existence for those units in the organisation where CONFIDENTIAL material does need to be regularly handled and processed as part of their business, eg, Serious Crime Analysis Section.

There is no National Standard for information assets which do not meet any of the criteria of the GPMS. Such assets will form the majority of the information processed within the NPIA on a daily basis. Whilst there is no mandatory requirement, the use of the marking "NOT PROTECTIVELY MARKED" shows that the originator has valued the data against the GPMS criteria and decided that it does not require protection.

**What happens if you apply too high a Protective Marking?**

If you apply too high a Protective Marking you may unnecessarily be limiting access to the asset, increasing the cost of the security controls needed for its protection and impairing the efficiency with which addressee organisations are able to conduct business.

Only the originator of a protectively marked asset may authorise its downgrading. Where the originating organisation has ceased to function, its successor becomes responsible. Where a successor cannot be traced, the holder of the asset may change its marking only in agreement with all other addressees.

It is important to remember that not all assets will require a Protective Marking, but those that do must be properly marked and handled.

### **What happens if you apply too low a Protective Marking?**

If you apply too low a Protective Marking you may put the asset at risk of accidental or deliberate compromise, since appropriate security controls may not be in place to provide adequate protection.

When deciding the level of Protective Marking you should apply, think about the asset's value in terms of the likely damage that could result from it falling into the wrong hands.

### **3.4.2 Process for assessing the Protective Marking**

The process of assessing the correct Protective Marking usually starts when a document, memo or other piece of information is created. Given however, that the GPMS covers all data and its transmission, it is equally important to consider Protective Marking before writing an email, faxing a document or even holding a conversation.

For example, let's assume that a document needs to be created:

- **Step 1** – Consider what is going to be in the document, who you would want to be able to see the document and who (if anyone) you wouldn't want to see it.
- **Step 2** – Review the Impact Level Definition Tables in [Annex A](#) for the appropriate business area(s), starting at Impact Level 6 and working down to Impact Level 0 for all sub categories, until you find the most likely Impact(s) of a worst case leakage of the information in the document you are about to create. Within NPIA Tables 2 & 4 are the most likely to be used. NB: there may be Impacts in a number of sub categories at different levels, so don't stop assessing when you find the first one.

- **Step 3** – Match the HIGHEST numbered Impact Level that you have found against the Protective Marking Table in [Annex B](#) to ascertain the correct Protective Marking for the document you are about to create.

**NB:** Within the NPIA ANY document containing “protected personal data” will attract an Impact Level of at least 1 – PROTECT. Specific guidance on how to assess “protected personal data” is contained within [Annex E](#)

- **Step 4** – Before creating the document check to ensure that:
  - If you are creating an electronic document, the network you are working on is Accredited to carry data at that Protective Marking. Remember that a majority of NPIA networks are only Accredited to carry data marked up to RESTRICTED.
  - If you are creating a typed or handwritten document, you have the necessary secure storage facilities for the relevant Protective Marking.
- **Step 5** – Consider whether you will need to apply a DESCRIPTOR to the Protective Marking – NB if the result at step 3 was Impact Level 1 or 2, ie a PROTECT Marking is required, then a DESCRIPTOR must be added. DESCRIPTORS are listed in [Annex C](#).
- **Step 6** – In some very rare instances a CODEWORD or NICKNAME may need to be applied to further protect the information, or a NATIONAL CAVEAT applied to limit information to particular Nationalities – if you feel that any of these may be likely, do not proceed any further without obtaining explicit advice from the Security & Business Continuity Unit!

- **Step 7** – Create the document ensuring that the Protective Marking and any DESCRIPTORS, CODEWORDS, NICKNAMES or NATIONAL CAVEATS are shown in bold font and in capital letters at the top and bottom of every page.
- **Step 8** – File, save or send the document according to the instructions appropriate for its Protective Marking. A summary of handling, transfer and disposal requirements up to CONFIDENTIAL is attached at [Annex D](#), for information on higher markings please contact the Security & Business Continuity Unit.

### **3.4.3 Layout and Labelling**

When creating documents, the Protective Marking (and any DESCRIPTORS) must be centrally placed in both Headers and Footers, in bold font and capital letters.

#### **Should all protectively marked assets be physically labelled?**

In the majority of instances protectively marked assets should be physically labelled. Where a sensitive asset is labelled with a Protective Marking and, if appropriate, special handling instructions, the marking and instructions should be noticeably displayed so that the degree of sensitivity is obvious to all.

Whilst the guidance given here relates more easily to documentary assets, recorded on physical storage media (eg, paper, floppy disks, optical and microform), it is important to remember that Protectively Marked information processed, stored and transmitted in electronic form needs to be similarly and appropriately protected.

#### **3.4.4 Protective Marking Responsibility**

The responsibility for deciding on the appropriate marking lies with the originator, and that decision should always be based on the anticipated impact of that particular information being compromised by whatever means, for instance it becoming public. Once the decision is made, the appropriate marking should be applied.

The decision should take full account of the GPMS criteria, as outlined in this policy, as these are set standards which must be applied consistently throughout Government and the Police Community.

#### **3.4.5 Change Process**

The originator retains responsibility for the Protective Marking throughout the lifetime of the information asset, and it is important to understand that the Protective Marking of that asset **cannot** be changed without the originator's agreement. (Should they be no longer available, their line manager should be consulted).

The Protective Marking of an asset may of course need to change during the lifetime of that asset, and regular reviews should be carried out by the originator to ensure that the Protective Marking is still valid; it may need to be changed up or down. Such reviews, and any decisions to change the Marking, should be carried out with close reference the GPMS criteria, as outlined in this policy.

### **3.5 Handling and Transfer**

The GPMS also sets strict criteria for the movement of Protectively Marked assets, and these are outlined within [Annex D](#).

## **3.6 Storage**

### **3.6.1 Electronic data**

The security of Protectively Marked electronic data requires storage at an appropriate level. The NPIA information systems (networks) will be Accredited at a particular level (usually RESTRICTED) and documents that require a higher Protective Marking must not be processed or stored on them. It is each individual's responsibility to ensure that they comply with the GPMS and the standards for the NPIA information system they are working on.

### **3.6.2 Physical assets**

Where the Protective Marking applies to a hard copy or other physical asset, the general rule for storage within a secure NPIA site is as follows:

- RESTRICTED – one physical barrier e.g. locked cabinet, cupboard or drawer.
- CONFIDENTIAL – two physical barriers e.g. locked cabinet etc in a locked room.
- SECRET & TOP SECRET – specialist advice should be sought from the NPIA Security & Business Continuity Unit.

More detailed guidance is available at [Annex D](#).

## **3.7 Disposal**

The disposal requirements for Protectively Marked assets will vary depending upon the Protective Marking of the asset and its physical form (eg, disposal requirements for a hard drive will differ significantly to those of a piece of paper). A summary of disposal standards is contained within [Annex D](#).

## **4. IMPLICATIONS OF THE POLICY**

### **4.1 Training Requirements**

Line managers must ensure that all employees for whom they are responsible read and understand the policy.

### **4.2 IT Infrastructure**

This policy does not require any input from IT to be implemented.

### **4.3 Related Policies**

[Asset Management Policy](#) (A.7)

[Secure Disposal or Re-Use of Equipment Policy](#) (A.9.2.6)

[Clear Desk and Screen Policy](#) (A.11.3.3)

## **5. MONITORING AND REVIEW**

This policy will be reviewed annually by the Senior Information Risk Manager and the relevant governance board, taking into account any feedback received or security incidents reported.

**ANNEX A - Impact Level Definition Tables**

**Table 1 - Defence, Intn'l Relations, Security and Intelligence**

Sub category	Impact Level						
	0	1	2	3	4	5	6
<b>Impact on life and safety</b>	None	None	Inconvenience or discomfort caused to an individual	Risk to an individual's personal safety or liberty	Risk to a group of individual's security or liberty	Threaten life directly leading to limited loss of life	Lead directly to widespread loss of life
<b>Impact on political stability</b>	None	None	None	Minor loss of confidence in Government	Major loss of confidence in Government	Threaten directly the internal political stability of the UK or friendly countries	Collapse of internal political stability of the UK or friendly countries
<b>Impact on military operations</b>	None	Delay to or loss of minor supply service	Loss of a number of minor supply services	Make it more difficult to maintain the operational effectiveness of security of UK or allied forces (eg compromise of UK forces doctrine or training materials)	Cause damage to the operational effectiveness or security of UK or allied forces (eg compromise of a logistics system causing re-supply problems without causing risk to life)	Cause severe damage to the operational effectiveness or security of UK or allied forces (eg compromise of the operational plans of units of company size or below in a theatre of military operations)	Cause exceptionally grave damage to the operational effectiveness or security of UK or allied forces (eg compromise of the operational plans of units of battalion size or above in a theatre of military operations)
<b>Impact on foreign relations</b>	None	None	None	Cause embarrassment to Diplomatic relations	Materially damage diplomatic relations (eg cause formal protest or other sanctions)	Raise International tension, or seriously damage relations with friendly governments	Directly provoke International conflict, or cause exceptionally grave damage to relations with friendly governments
<b>Impact on International trade negotiations</b>	None	None	None	Disadvantage a major UK Company	Disadvantage a number of major UK Companies	Disadvantage the UK in International negotiations (eg advance compromise of UK negotiation strategy or	Severely disadvantage the UK in International negotiations (eg advance compromise of UK negotiation strategy or

**NOT PROTECTIVELY MARKED**

						acceptable outcomes, in the context of a bilateral trade dispute)	acceptable outcomes, in the context of a major EU or WTO negotiating round)
<b>Impact on intelligence operations</b>	None	None	None	Damage unique intelligence operations in support of intelligence requirements at JIC Priority Three or less	Halt unique intelligence operations in support of intelligence requirements at JIC Priority Three or less, or damage unique intelligence operations in support of intelligence requirements at JIC Priority Two	Halt unique intelligence operations in support of intelligence requirements at JIC Priority Two, or damage unique intelligence operations in support of intelligence requirements at JIC Priority One	Halt unique intelligence operations in support of intelligence requirements at JIC Priority One

• **Table 2 – Public Order, Safety and Law Enforcement**

Sub category	Impact Level						
	0	1	2	3	4	5	6
<b>Impact on life and safety</b>	None	None	Inconvenience or cause discomfort to an individual	Risk to an individual's personal safety or liberty	Risk to a group of individual's security or liberty	Threaten life directly leading to limited loss of life	Lead directly to widespread loss of life
<b>Impact on provision of emergency services</b>	None	Minor disruption to emergency service activities that requires reprioritisation at the local (eg police station) level to meet	Minor disruption to emergency service activities that requires reprioritisation at the area or divisional level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the county or organisational level to meet expected levels of service	Disruption to emergency service activities that requires reprioritisation at the national level (eg one or more police force requesting help from another) to meet expected levels of service	Disruption to emergency service activities that requires emergency powers to be invoked (eg military assistance to the emergency services) to meet expected levels of service	Threaten directly the internal stability of the UK or friendly countries leading to widespread instability

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**NOT PROTECTIVELY MARKED**

		expected levels of service					
<b>Impact on crime fighting</b>	None	None	Hinder the detection of low-level crime (ie crime not defined as "serious crime")	Impede the investigation of, or facilitate the commission of low-level crime (ie crime not defined as "serious crime"), or hinder the detection of serious crime	Impede the investigation of, or facilitate the commission of serious crime (as defined in legislation)	Cause major, long-term impairment to the ability to investigate serious crime (as defined in legislation).	Cause major, long-term impairment to the ability to investigate serious organised crime (as defined in legislation)
<b>Impact on judicial proceedings</b>	None	None	Minor failure in local Magistrates courts	Cause a low-level criminal prosecution to collapse; cause a conviction for a low-level criminal offence to be declared unsafe or referred for appeal	Cause a serious crime prosecution to collapse; cause a conviction for a serious criminal offence to be declared unsafe or referred for appeal	Cause a number of criminal convictions to be declared unsafe or referred to appeal (eg through persistent and undetected compromise of evidence-handling system)	Collapse of the UK Judicial system

• **Table 3 – Trade, Economics and Public Finances**

Sub category	Impact Level						
	0	1	2	3	4	5	6
<b>Impact public finances</b>	Minor impact (eg cost of sundries)	Cause a loss to Public Sector of up to £1,000	Cause a loss to Public Sector of up to £10,000	Cause a loss to HMG/Public Sector of up to £1 million	Cause a loss to HMG/Public Sector of up to £10 million	Cause short term material damage to national finances or economic interests (to an estimated total up to £100 million)	Cause major, long term damage to the UK economy (to an estimated total in excess of £100 million)

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**NOT PROTECTIVELY MARKED**

<b>Impact on UK trade and commerce</b>	None	None	Undermine the financial viability of a number of UK SME's	Undermine the financial viability of a minor UK-based or UK-owned organisation	Undermine the financial viability of a major UK-based or UK-owned organisation	Cause material damage to international trade or commerce, directly and noticeably reducing economic growth in the UK	Cause major, long term damage to global trade or commerce, leading to prolonged recession or hyperinflation in the UK
--	------	------	---	--	--	--	---

▪ **Table 4 – Public Services: impacts, disruption, compromise, etc**

Sub category	Impact Level						
	0	1	2	3	4	5	6
<b>Risk to life and safety (particularly medical services)</b>	None	None	Likely to cause discomfort to an individual	Likely to risk any party's personal safety	Likely to cause serious injury or illness to any party	May cause a direct threat to life leading to limited loss of life	May lead directly to widespread loss of life
<b>Impact on the provision of the service (independent of risks to life and safety)</b>	None	Likely to affect a single citizen	Likely to affect many citizens	Likely to require active management at the county or authority level to meet expected levels of service	Likely to require active management at the national level to meet expected levels of service	May require emergency powers to be invoked or emergency assistance rendered to meet expected levels of service	May lead to complete breakdown in public services, with critical impact on the continuity of government
<b>Inconvenience and impact on public confidence in public services</b>	May cause minor inconvenience to an individual citizen (eg a	Likely to reduce an individual citizen's perception of that service	Likely to reduce the perception of that service by many citizens (eg compromise leading to an outpatient	Likely to result in undermined confidence in the service provider generally (eg public failures at a hospital leading to a noticeable	Likely to result in undermined confidence in the service at a national level (eg compromise of national patient information databases	May lead to a loss of public trust in the service severe enough to cause a noticeable drop in citizens using the service through mistrust, with the	May lead to a complete breakdown in public trust, black market services thrive, consequent widespread loss of life or critical impact on continuity

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**NOT PROTECTIVELY MARKED**

	short delay in applying for a non-essential government service)	(eg a compromise leading to the cancellation of a hospital appointment)	clinic closing for a day, with cancellation of multiple appointments)	lower public confidence in that hospital)	leading to undermined confidence in the NHS)	consequent risk to life	of government
<b>Impact on public finances</b>	None	Likely to cause a loss to the Public sector of up to £1,000	Likely to cause a loss to the Public sector of up to £10,000	Likely to cause a loss to HMG/Public sector of up to £1 million	Likely to cause a loss to HMG/Public sector of up to £10 million	May cause short-term material damage to national finances or economic interests (to an estimated total up to £100 million)	May cause major, long-term material damage to the UK economy (to an estimated total of over £100 million)
<b>Impact on non-public finances</b>	Likely to have minimal impact (eg cost of sundries)	Likely to cause minor financial loss to any party (eg loss of <£100 for an individual or sole trader, loss of <£1,000 for a larger business or organisation)	Likely to cause moderate financial loss to any party (eg loss of up to £1,000 for an individual or sole trader, loss of up to £10,000 for a larger business or organisation)	Likely to cause substantial financial loss to any party (eg loss of up to £10,000 for an individual or sole trader, loss of up to £100,000 for a larger business or organisation)	Likely to cause substantial financial loss to any party (eg loss of up to £100,000 for an individual or sole trader, loss of up to £1 million for a larger business or organisation)	May cause major financial loss to any party (eg loss of up to £1 million for an individual or sole trader, loss of up to £10 million for a larger business or organisation)	May cause extensive financial loss to any party (eg loss of up to £10 million for an individual or sole trader, loss of up to £100 million for a larger business or organisation)
<b>Distress to the public</b>	None	None	Likely to cause short-term distress to an individual citizen	Likely to cause prolonged distress for an individual citizen, or short-term distress for many citizens	Likely to cause prolonged distress for many citizens	Likely to cause widespread panic and severe disruption to public order	May cause collapse of internal political stability of the UK or friendly countries
<b>Damage to</b>	None	None	Likely to cause	Likely to cause loss of	Likely to cause	Likely to cause long-term	Likely to cause major,

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**NOT PROTECTIVELY MARKED**

<b>standing or reputation</b>			embarrassment to an individual citizen or organisation	reputation for an individual citizen or organisation	embarrassment or loss of reputation for many citizens or organisations	(eg months) or permanent loss of reputation for many citizens or organisations	long-term damage to the UK population
<b>Locally provisioned services with an impact on the personal safety of citizens (eg sheltered accommodation )</b>	None	None	Risk to any party's personal safety (eg compromise of address of a victim of abuse now in sheltered housing, where it is assessed that there is a low risk of further abuse if such information became known to the original perpetrator)	Risk to any party's personal safety (eg compromise of address of a victim of abuse now in sheltered housing, where it is assessed that there is a moderate risk of further abuse if such information became known to the original perpetrator)	Serious risk to any party's personal safety (eg compromise of address of a victim of abuse now in sheltered housing, where it is assessed that there is a high risk of further abuse if such information became known to the original perpetrator)	Threaten life directly and leading to a limited loss of life (eg compromise of address of a victim of abuse now in sheltered housing, where it is assessed that there is a real risk of attempted murder)	Cause disruption to public services (particularly social care and environmental health services) on a scale likely to lead to widespread loss of life
<b>Locally provisioned services with an impact on the health of citizens (eg waste disposal)</b>	None	Disruption, compromise or flawed working of a local service which could pose a risk to health	Disruption, compromise or flawed working of a local service which could pose an increased risk to health (eg spread of disease)	Authority-wide disruption, compromise or flawed working of services which could pose an increased risk to health (eg spread of disease)	Significant authority-wide disruption, compromise or flawed working of services which could lead to major health risks	Major disruption or compromise of a Local Authorities services, or critical faults within these services, which could lead to severe health risks and limited loss of life	Catastrophic disruption or compromise of a number of Local Authority services, or catastrophic faults within these services, which could lead to severe health risks and widespread loss of life
<b>Locally provisioned services with no impact on health or safety of citizens (eg</b>	Trivial or no impact	Cancellation of services to a small number (up to 10) of citizens (eg closure of a	Cancellation of services to a number (up to 100) of citizens (eg closure of a library or other facility	Cancellation of multiple services to a number (up to 1,000) of citizens leading to financial losses (up to £1,000)	Loss of major services provided by Local Authorities leading to major financial losses (up to £100,000) to Local Authority and citizens	Total loss of major services provided by Local Authorities leading to major financial losses (up to £1 million) to Local Authority and citizens	Total loss of major services provided by a number of Local Authorities leading to severe financial losses (>£10 million) to the Local Authorities and a large

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**NOT PROTECTIVELY MARKED**

<b>library, land use and planning services)</b>		library or other facility)					number of citizens
<b>Locally provisioned services in support of the Civil Contingencies Act</b>	Trivial or no impact	Isolated or minor incident to which a Local Authority is not able to react within a few days which affects a small number of citizens	Isolated or minor incident to which a Local Authority is not able to react within a few days which affects a number of citizens/local businesses	Significant incident to which a Local Authority is not able to react within 24 hours which affects a large number of citizens/local businesses – eg significant flooding, fire, contamination or explosion	Major incident to which a Local Authority is not able to react within 24 hours which affects a large number of citizens/local businesses eg major flooding, fire, contamination, explosion or CNI failure	Major incident to which a Local Authority is not able to react within 12 hours which affects a large number of citizens/local businesses eg major flooding, fire, contamination, explosion or CNI failure	Major incident to which several Local Authorities are not able to react within 12 hours which affects a large number of citizens/local businesses eg major flooding, fire, contamination, explosion or CNI failure

**Table 5 – Critical National Infrastructure (CNI)**

Sub category	Impact Level						
	0	1	2	3	4	5	6
<b>Communications</b>	Trivial or no impact	Local loss of telecoms for a few hours	Local loss of telecoms for up to 12 hours	Local loss of telecoms for up to 24 hours	Loss of telecoms of a region for up to 24 hours	Local loss of telecoms nationally for up to a week	Local loss of telecoms nationally for more than a week
<b>Power</b>	Trivial or no impact	Local outages causing disruption for up to 12 hours	Local outage causing disruption for up to 24 hours	Loss of power in a region causing disruption for up to 24 hours	Loss of power in a region causing disruption for up to a week	Loss of power in a region causing disruption for more than a week	Loss of power nationally affecting the whole of the UK for more than a week
<b>Finance</b>	Trivial	Minimal impact (<	Minor loss to a	Major loss to a Leading	Major loss to a Leading	Severe losses to UK	Severe financial losses to

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**NOT PROTECTIVELY MARKED**

	or no impact	£10,000)	Financial Company (less than £1 million)	Financial Company of £millions	Financial Company of £10s millions	Business of up to £1 billion	UK Business of £10s billions
<b>Transport (NB Data based on the National Risk Assessment Impact Scale)</b>	Trivial or no impact	Minor disruption of a key local transport system for up to 12 hours	Minor disruption of a key local transport system for up to 24 hours	Disruption of a number of key local transport systems for up to 24 hours	Major disruption of key regional transport systems for up to a week	Severe national disruption of key transport systems for up to a week	Severe national disruption of key transport systems for over a month
<b>Water and Sewage</b>	Trivial or no impact	Breakdown of local water supplies and/or sewage service for a small number (<10) of people for more than a day	Breakdown of local water supplies and/or sewage services for a small number (<50) of people for more than a week	Breakdown of local water supplies and/or sewage services for a number (up to 100) of people or prolonged drought (up to 1 month)	Breakdown of local water supplies and/or sewage services for over a 100 people or prolonged drought (up to 1 month)	Breakdown of regional water supplies and/or sewage services (affecting > 100 people) or prolonged drought (up to 3 months)	Total breakdown of national water supplies and/or sewage services (affecting > 100 people) or prolonged drought (>6 months)
<b>Food and consumable</b>	Trivial or no impact	Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food for up to a week	Local disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food for up to a month	Regional disruption to the distribution of some essential goods, fuel, raw materials, medicines and/or food for up to a week	Regional disruption to the distribution of some essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month	National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for up to a month	National disruption to the distribution of essential goods, fuel, raw materials and medicines and widespread disruption of food for over a month

**NOT PROTECTIVELY MARKED**

(This is a non-contractual policy and may be varied by the NPIA at will)

**ANNEX B - Protective Marking Table**

<b>Impact Level</b>	<b>Protective Marking</b>
<b>0</b>	<b>NOT PROTECTIVELY MARKED</b>
<b>1 &amp; 2</b>	<b>PROTECT</b>
<b>3</b>	<b>RESTRICTED</b>
<b>4</b>	<b>CONFIDENTIAL</b>
<b>5</b>	<b>SECRET</b>
<b>6</b>	<b>TOP SECRET</b>

**ANNEX C - Table of Descriptors**

**Do you need to apply a DESCRIPTOR relating to or concerning:**

**DESCRIPTOR to Use**

Actual or potential appointments yet to be announced?	<b>APPOINTMENTS</b>
Proposed or actual Budget measure before its announcement?	<b>BUDGET</b>
A commercial undertaking's progress or affairs?	<b>COMMERCIAL</b>
Tender consideration and the terms of tenders accepted?	<b>CONTRACTS</b>
Actual or potential award of an honour before it is announced?	<b>HONOURS</b>
Investigations into disciplinary or criminal matters?	<b>INVESTIGATION</b>
Policy and planning affecting the interests of groups of employees?	<b>MANAGEMENT</b>
Medical reports and records and material relating to them?	<b>MEDICAL</b>
Material only to be seen by the individual to whom it addressed?	<b>PERSONAL*</b>
Proposals for new or changed government policy before publication?	<b>POLICY</b>
Material which has come into the possession of government depts or agencies in the course of carrying out statutory regulatory duties?	<b>REGULATORY</b>
Information that contains references to names of identifiable employees	<b>STAFF</b>
Details of visits by, for example, royalty or very senior individuals?	<b>VISITS</b>

**\*PERSONAL** may be applied without a Protective Marking

**ANNEX D - Summary of Handling, Transfer & Disposal Requirements**

<b>Application/ Activity</b>	<b>PROTECT</b>	<b>RESTRICTED</b>	<b>CONFIDENTIAL</b>
<b>Marking of Documents</b>	In capitals & bold on the top & bottom of every page.	In capitals & bold on the top & bottom of every page.	In capitals & bold on the top & bottom of every page.
<b>Storage of hard copy documents</b>	Protected by one barrier, eg locked container within a secure building.	Protected by one barrier, eg locked container within a secure building.	Protected by two barriers, eg locked container within a locked room within a secure building.
<b>Disposal of paper waste</b>	Shred or use secure waste sacks. Keep sacks secure when left unattended.	Use a cross cut shredder or secure waste sacks. Keep sacks secure when left unattended.	Use a SEAP approved cross cut shredder or other secure approved waste sack procedure.
<b>Disposal of magnetic media</b>	Refer to Secure Disposal or Re-Use of Equipment Instructions.	Refer to Secure Disposal or Re-Use of Equipment Instructions.	Refer to Secure Disposal or Re-Use of Equipment Instructions.
<b>Re-Use of Media (Hard Drives etc)</b>	Refer to Secure Disposal or Re-Use of Equipment Instructions.	Refer to Secure Disposal or Re-Use of Equipment Instructions.	Refer to Secure Disposal or Re-Use of Equipment Instructions.
<b>Movement within single NPIA site or between NPIA sites using own distribution system, (ie must not pass out of hands of NPIA staff)</b>	In a sealed envelope with Protective Marking shown. A transit envelope <b>may</b> be used if sealed with a security label.	In a sealed envelope with Protective Marking shown. A transit envelope <b>may</b> be used if sealed with a security label.	In a new sealed envelope with Protective Marking shown. Transit envelopes must not be used.

**Annex D - Cont'd**

<b>Application/ Activity</b>	<b>PROTECT</b>	<b>RESTRICTED</b>	<b>CONFIDENTIAL</b>
<b>Movement outside of NPIA sites (eg to forces or partner agencies)</b>	By post or courier in a sealed envelope. Do not show Protective Marking on the envelope.	By post or courier in a sealed envelope. Do not show Protective Marking on the envelope.	By post or courier. Double enveloped, both fully addressed. Protective Marking shown on inner envelope only. Return address on outer envelope.
<b>NPIA Internal Phone Network</b>	May be used.	May be used if private, secure network.	May be used if private, secure network in cases of urgency.
<b>Public Telephone, Mobile Telephone and WAP 'phone networks</b>	May be used.	May be used in cases of urgency if due caution is exercised.	Not to be used.
<b>Pager systems and SMS</b>	May be used.	Not to be used.	Not to be used.
<b>Facsimile machines</b>	May be used.	May be used in cases of urgency if due caution is exercised.	Not to be used unless approved encrypted service is available.
<b>Airwave Radios</b>	May be used.	May be used.	Not to be used unless enhanced end to end encryption service deployed.
<b>NPIA IT Network. Email services using PNN, GSI and other approved secure addressing conventions</b>	May be used.	May be used.	Not to be used unless approved encrypted service is available.
<b>Internet Email/Internet services</b>	May be used.	Not to be used unless approved encrypted service is available.	Not to be used unless approved encrypted service is available.

**ANNEX E – Minimum Scope of Protected Personal Data**

Departments must identify data they or their delivery partners hold whose release or loss could cause harm or distress to individuals. This must include as a minimum all data falling into one or both categories below:

**A. Any information that links one or more identifiable living persons with information about them whose release would put them at significant harm or distress.**

1. one or more of the pieces of information which can be used along with public domain information to identify an individual	combined with	2. information about that individual whose release is likely to cause harm or distress
<p>Name / addresses (home or business or both) / postcode / email / telephone numbers / driving licence number / date of birth.</p> <p>[NB: Driving licence number is included because it directly yields d.o.b. and first part of surname]</p>		<p>Sensitive personal data as defined by s2 of the Data Protection Act, including records relating to the criminal justice system and group membership.</p> <p>DNA or finger prints / bank, financial or credit card details / mother’s maiden name / NI number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing.</p>

These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category.

**B. Any source of information about 1,000 or more identifiable individuals, other than information sourced from the public domain.**

This could be a database with 1,000 or more entries containing facts mentioned in box 1, or an electronic folder or drive containing 1,000 or more records about individuals. Again, this is a minimum standard. Information on smaller numbers of individuals may warrant protection because of the nature of the individuals, nature or source of the information, or extent of the information.