NHS
Counter Fraud Authority

Data Handling, Storage, Retention and Records Management Policy

September 2018

Version:2.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Version control

Version	Name	Date	Comment
2.0	Trevor Duplessis	September 2018	Update

Table of Contents

1. Introduction

1.1 While information held by the NHS Counter Fraud Authority (NHSCFA) represents some of the organisation's most valuable assets; disposal scheduling is an equally important aspect of establishing and maintaining control of corporate information, as not all information should be retained indefinitely.

1.2 The General Data Protection Regulations (GDPR), the Data Protection Act 2018 and the Freedom of information Act 2000, impose stringent duties on public sector organisations with regard to robust records management practices. Therefore it is essential that all information is not only used, communicated, transferred and stored in a manner that complies with the broader information management and security framework of NHSCFA, but also ensures that the final disposal of records is undertaken in accordance with legislation and key guidance, such as the Records Management Code of Practice for Health and Social Care 2016.

1.3 The appropriate handling, storage and disposal of information is the responsibility of all NHSCFA members of staff. The organisational processes in place to facilitate this will be ineffective unless the correct procedures are carried out in a careful and consistent manner.

1.4 NHSCFA is committed to properly protecting the information that it holds. This policy and associated practices and procedures have been agreed by the NHSCFA Board.

2. Purpose and scope

2.1 This policy sets out the principles governing the retention and disposal of information so that records are not kept longer than they are needed, in compliance with the Department of Health and Social Care Unit's 2016 records management code of practice and supplementing the organisation's policies relating to information governance and security management.

2.2 The policy is to be read in conjunction with NHSCFA's policies on:

- Information Governance
- Information Security Management
- Acceptable Use
- Data protection

- Mobile Computing
- Government Security Classification guidance

2.3 The policy is concerned with all information systems, digital and non-digital and will cover all information within NHSCFA that is or may be:

- stored on computers
- transmitted across networks
- printed out or written on paper
- sent internally or externally (by whatever method)
- stored on removable and other electronic media

2.4 The policy applies to all business units within NHSCFA and as appropriate to its contractors and any third-party service providers.

3. Responsibilities

3.1 NHSCFA Board

The Board is ultimately responsible for ensuring that the organisation meets its legal responsibilities and the adoption of internal and external governance requirements. These responsibilities include maintaining standards of information governance which ensure the quality of record keeping and record management.

The Board will be informed of any issues via the Board Assurance Framework report, which the Information Governance Lead will feed into.

3.2 Chief Executive

The chief executive has overall responsibility for records management in the organisation. As accountable officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

Operational responsibility for information governance is delegated by Chief Executive to the Information Governance Lead.

3.3 Caldicott Guardian

NHSCFA's Caldicott Guardians have particular responsibility regarding the use of person identifiable information. The organisation's Guardians have overall responsibility for ensuring person identifiable information is shared in an appropriate and secure manner.

The duties and responsibilities of the Caldicott Guardians are outlined in NHSCFA's Caldicott Guardian Policy.

3.4 Information Governance Lead

The Information Governance Lead is responsible for providing records management advice to the organisation, co-ordinating implementation and monitoring compliance with this policy.

Compliance will be monitored through audits of business unit practices by the delivery of appropriate Governance and Assurance exercises team and computer based training assessments, on knowledge and awareness of organisational policies, procedures and best practice.

3.5 Business Unit Managers

The responsibility for local records management is devolved to department heads who retain overall responsibility for the management of records received and used in their activities. The creation of appropriate 'Standard Operating Procedures (SOPs), will ensure that records created within their units are managed in a way which meets the aims of the organisation's record management policies.

Unit managers must ensure that their staff are adequately trained in records management and ensure compliance with the data handling policy and associated good practice guidance.

3.6 Staff

All staff whether permanent, temporary and contracted or contractors, who receive, create and use records will have record management responsibilities. They must make sure that they keep appropriate records of their work and manage those records not only in keeping with this policy, the business unit's SOPs, associated and supplemental guidance but also in line with any relevant legislation. They will also need to adhere to any recommended governance and assurance actions.

4. Security classification of information

4.1 Information created and received by NHSCFA should be classified according to the sensitivity of its contents. Classification and controls should take account of the organisation's needs for sharing or restricting information, together with any

associated impacts and risks such as unauthorised access or damage to the information[1].

4.2 The classification scheme is part of the overall concept of NHSCFA Information Security and its proper use is essential to the proper conduct of document movement. A failure to accord a document the appropriate classification could result in the compromise of NHSCFA assets or operations and a misuse of resources.

4.3 It is the responsibility of the person producing the document to assign a classification level. This person is known as the 'Originator', and is usually the author of the document. The Originator decides on the appropriate classification level for the document based upon an assessment of the sensitivity of its content and the impact of its compromise

4.4 The single protective marking should be clearly given at the top and bottom of every page of every document. It should be positioned in the centre of the page and should be in BLOCK CAPITALS.

4.5 If documents are page numbered and the page number is positioned at the bottom of the page, it should be placed above the protective marking. For a document with a centre positioned page number, the footer will look as follows:

(page number #)
PROTECTIVE MARKING

4.6 The classification used within the NHSCFA for all information is **OFFICIAL**. Information classified as OFFICIAL includes non-sensitive information, such as the following non-exhaustive list:

- routine correspondence where there is no confidentiality requirement.
- circulars
- bulletins
- guidance
- news/press releases

4.7 There may occasionally be a requirement to protect the integrity and the availability of information, such as transactional information - one-off exchanges with third parties including members of the public which may include personal, commercial or financial information.

4.8 There is a requirement to protect the confidentiality, integrity and availability of this type of information to avoid disruption to service delivery, commercial or financial impact. For example routine NHSCFA business such as:

[1] See also Classification system guidelines for NHS Protect information assets (documents) guide

- routine correspondence with third parties and members of the public which may contain some personal or commercial information
- non person-identifiable information
- inter-office memoranda
- Internal phone directories

There is also a legal requirement to protect person identifiable and sensitive information as defined by the GDPR and the Data Protection Act 2018.

4.9 Consequences if OFFICIAL information is mishandled:

- Unauthorised disclosure would not significantly impact NHSCFA or any of its stakeholders, including members of the public, or employees.
- Protective Marking - there is no requirement to explicitly mark routine OFFICIAL information.

4.10 There is a subset of information handled by the NHSCFA where the inappropriate use of the information could have damaging consequences for the organisation, for an individual (or groups), or other organisations. This information, which is caveated **OFFICIAL-SENSITIVE**, includes:

- personal and/or patient identifiable information
- staff personnel file and/or Electronic Staff Records (ESR)
- staff pay and expenses
- antecedent records
- information about investigations, civil or criminal proceedings that could compromise enforcement activities or prejudice court cases
- legal advice/opinions
- risk registers
- extremely sensitive NHSCFA corporate or operational information, such as major security or business continuity issues

4.11 Consequences if OFFICIAL-SENSITIVE information is mishandled:

- Unauthorised disclosure likely to result in significant adverse impact, embarrassment or penalties to NHSCFA, its stakeholders, employees, or members of the public.

- Protective Marking - where there is a clear and justifiable requirement to reinforce a “need to know” basis, information should be conspicuously marked OFFICIAL-SENSITIVE.

See Appendix 1.

5. Downgrading/Re-grading document

5.1 The originator is responsible for giving a document its protective marking and the responsibility for changing that marking lies solely with the originator. Recipients must not re-grade a document without reference to, and the agreement of, the originator. Should a recipient wish to challenge a document’s protective marking, they should approach the originator.

5.2 Where it is agreed to re-grade a document, all recipients of the document should be informed of the re-grading. This will avoid different offices holding copies of the same document with different protective markings.

5.3 If the original originator is not available (due to staff changes, etc) the request for down/re-grading should be sent to the originating office. Compliance with the business unit’s SOPs together with a clear rationale for the reclassification of a document should be included in the ‘Version Controls’ comments section.

6. Information access

6.1 Internal and external access to information held by the NHSCFA and to the systems within which they are held is governed by the security classification of the information.

- Official information is either generally available to the public or all staff on a need-to-know basis, as determined by their line manager

- Official-Sensitive information should only be available to staff who have a business need for the information and such access rights should be capable of being monitored and revised.

6.2 Where access to Official Sensitive information has been authorised, use of such data shall be limited to the purpose required to perform NHSCFA business.

6.3 Where a member of staff who has access to Official-Sensitive information either leaves the organisation’s employ or has their authorisation removed e.g. as a result of a secondment or a change of role, their access status must be updated accordingly as soon as practicable.

6.4 The distribution of documents should be confined to those who have a clear need-to-know. Where appropriate document should contain a distribution list, detailing whether it has been made available internally, externally or both.

7. Transfer and exchange of information

7.1 Information and data can be transferred and exchanged in a variety of ways, directly and indirectly. These may include:

- spoken word
- post, fax, or e-mail
- internet or intranet
- magnetic media (including but not limited to CDs, DVDs, Memory Sticks)
- electronic file transfers and document sharing
- web portals (i.e. NHSCFA web-enabled applications)

7.2 Information must only be transferred to persons who are authorised to have access to it and there should be adequate security measures in place at the virtual or physical destination. Where Official-Sensitive information is being transferred, Information Asset Owners should seek additional assurances around the security measures in place.

7.3 Official-Sensitive information should not be sent or physically taken off-site without appropriate authorisation by the Information Asset Owner (or their delegated deputy) and appropriate security measures in place, such as encryption.

7.4 The recommended use of the various methods of transferring information is set out in the NHSCFA Data Classification Matrix, which should be adhered to at all times. See Appendix 2

7.5 The transfer and exchange of information concerning identifiable living persons will additionally be subject to NHSCFA's GDPR - Data Protection Policy.

8. Storage and protection of information

8.1 Information in all formats should be stored throughout its existence in an environment suited to its format and security classification, to protect it from threats to its physical integrity through unnecessary wear and tear, physical harm, specific risks such a fire, flooding or extreme environmental fluctuations and security from loss or unauthorised access.

8.2 Information whether original or duplicate, should never be kept outside of corporate systems, such as on PC hard drives or other removable media, except where necessary for example a temporary off-line copy because of a business need to work off-site or off-line or for an authorised transfer.

8.3 Information should be stored in systems and according to classifications, frameworks and procedures that enable it to be readily identified and retrieved throughout its existence.

8.4 Information held in digital formats should be managed and stored in such a way as to ensure usability and accessibility throughout its lifetime. This may involve migration of information between environments and systems, conversion to updated software versions, or from obsolete to current formats.

8.5 Protection from unauthorised access may require mechanisms such as password-protection or encryption of digital files and data or sign-in request sheets for access to non-digital information.

8.6 Where information is stored on a mobile device (PDA, laptop, USB drive), special care must be taken to ensure that the device is protected from theft, loss, or damage, particularly if it is transferred or used away from NHSCFA sites.

8.7 Physical access to information should be appropriately restricted by securing it in rooms, cabinets, drawers or other storage areas and by ensuring that files and computer monitors are not left open and unsecured to general or casual view.

8.8 Individuals are personally responsible for those documents in their care.

9. Retention and disposal of information

9.1 The retention periods for all of the categories of information held by the NHSCFA is set out in the organisation's Data Retention Schedule[2]. This applies to information (originals and duplicates) in all formats and systems.

[2] 2016

9.2 Information may be subject to one of a number of disposal actions at the end of its permitted life cycle. Typical disposal actions include:

- internal archive
- transfer and archive at an external storage facility
- destruction
- deletion

9.3 Information should only be destroyed in the ordinary course of business, in accordance with the periods stipulated in the Data Retention Schedule. No information subject to ongoing or pending investigations, audit, or litigation should be destroyed.

9.4 Physical destruction of digital (and any applicable non-digital) investigation material will be carried out in accordance with the Forensic Computer Unit's (FCU) Standard Operating Procedures [insert link]. All other digital material will be deleted or destroyed in accordance with ISA/Capita's documented procedures.

9.5 Where electronic data is to be erased but the medium left intact, it must be deleted to the extent appropriate to the security classification. The destruction processes appropriate to each security classification, for information held in digital or non-digital formats, are set out in the NHSCFA Data Classification Matrix.

10. Exception for Intelligence Information

10.1 What is intelligence Information?

Intelligence information can be described as the 'product' resulting from the collection, evaluation and analysis of all information acquired and provided, in respect of specified operational organisational objectives.

10.2 The retention periods for all categories of information held by NHSCFA are set out in the organisation's Data Retention Schedule. The exception to this is information relating to any behaviour, method of operation or unusual practices, linked to potential offences of fraud, bribery or corruption within the NHS and wider health service, that cannot be immediately linked to an identifiable individual(s). This information may be retained for a period beyond those currently set out in the Data Retention Schedule ***subject to regular reviews*** while additional information and/or identifiers are sought.

11. Reporting of incidents

11.1 Any incident involving the suspected loss or compromise of any protectively marked material or person-identifiable data must be reported immediately, in accordance with the NHSCFA's Information Breach Reporting policy.

12. Validity of this policy

12.1 Associated data handling and storage standards will be reviewed at least annually (or as and when, if new legislation, codes of practice or national standards are introduced).

Appendix 1

Government Security Classifications
FAQ Sheet 3: Working with Personal Information
v1.0 - April 2013

This FAQ sheet addresses practical aspects of working with personal information and data using the Government Security Classifications Policy (December 2012). It is intended to support a consistent approach to implementation that can ensure trust, interoperability and effective sharing.

Will all personal information be handled in OFFICIAL?

Almost all personal information/data will be handled within OFFICIAL without any caveat or descriptor. In very limited circumstances, specific sensitivity considerations may warrant additional (generally procedural) controls to reinforce the 'need to know' for access to certain personal data at OFFICIAL.

Personal information / data should only be managed in the SECRET classification where the context warrants defending against a heightened threat profile, e.g. data identifies a person as being in an exceptionally sensitive position or situation (e.g. an employee of the Security and Intelligence Agencies).

What about sensitive personal data as defined by the Data Protection Act (DPA)?

In most cases (apart from where other particular sensitivity considerations apply) personal information and sensitive data, as defined by the General Data Protection Regulations (GDPR) or the Data Protection Act (DPA) 2018, will be handled within OFFICIAL without any caveat or descriptor. This also applies to information previously marked protected personal data as defined in HMG Information Assurance Standard 6.

Will personal information in the OFFICIAL level be widely accessible?

No. All information must be subject to appropriate protection. There is no presumption of unbounded access at any level of the classification policy; though the principles of openness, transparency and information reuse need to be considered. As with current arrangements, organisations should use ICT access control measures, supported by procedural and personnel controls, to manage their information assets and enforce the 'need to know' principle.

All personal data / information is subject to the 'need to know' principle and it is the responsibility of Information Asset Owners (IAOs) to ensure that this is enforced in respect of personal data / information for which they are responsible.

Will the OFFICAL level provide the adequate/proper protection for personal data?

Everyone working with government information, staff, contractors and service providers, has a personal responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not.

IAOs need to consider the sensitivity and threats to their information and to identify those instances where access to personal information must be no wider than necessary for the efficient conduct of an organisation's business. The „need to know" principle must be used wherever personal information is collected, stored, processed, destroyed or shared within government and when dealing with external public or private sector organisations, and effective procedural controls put in place.

The recommended technical controls for the OFFICIAL classification set out in the GSC Security Controls Framework provide an appropriate level of protection for most personal information and data held on ICT systems. However, the onus remains on IAOs and business leads to properly understand the value, sensitivity and threats to their information when determining the Confidentiality, Integrity and Availability requirements for specific ICT solutions.

Technical controls at OFFICIAL utilise 'good' commercial ICT products and services. Whilst these controls cannot absolutely assure against the most sophisticated highly capable, determined and well resourced threats, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access this information. This is no different from current arrangements for the lower classification level systems.

Is there a single set of baseline security controls that will protect all personal data?

No, as currently the controls will vary according to a range of factors, for example the value and sensitivity of the information, the threats to that information, how it is used, by whom and where. Organisations need to undertake an holistic risk assessment to determine the appropriate controls necessary to meet the confidentiality, integrity and availability requirements.

What about meeting the Data Protection Act requirements?

The DPA requirement to provide appropriate and proportionate protection for personal data is unchanged. Senior Information Risk Owners (SIROs) and IAOs need to assure themselves that they have taken reasonable steps to comply with the DPA principles. Organisations must ensure that staff are trained in the handling of any personal data they process or manage and that tailored guidance is available about specific local processes. Security Classifications are designed to be used in parallel with any DPA controls but will not in themselves provide the requisite protection for information covered by DPA.

What type of personal information might qualify as OFFICIAL-SENSITIVE?

The OFFICIAL-SENSITIVE caveat should be applied where the 'need to know' must be most rigorously enforced, particularly where information may be being shared outside of a routine or well understood business process. For example, where the loss or compromise of information could have severely damaging consequences for an individual or group of individuals - there is a clear and justifiable requirement to reinforce the 'need to know principle' particularly rigorously across the organisation.

To maintain its currency the threshold for marking information OFFICIAL-SENSITIVE should be kept quite high. It is certainly not intended that because an OFFICIAL document or data contains personal information it should be routinely marked OFFICIAL-SENSITIVE, it should meet the criteria set out above.

Aggregation of large amounts of personal data has no bearing on the application of classification markings, but it can change the threat to the information and also enhance the impact of any compromise. Where large data sets of personal information exist in the OFFICIAL classification, effective procedural, and in some cases technical, controls may be appropriate to reinforce the „need to know" principle and provide enhanced protection. However the data should not be marked OFFICIAL-SENSITIVE.

Who decides what information is OFFICIAL-SENSITIVE?

Organisations" SIROs and IAOs, need to make their own judgements about the value and sensitivity of the information that they manage, and decide the instances where it is appropriate to use the OFFICIAL-SENSITIVE caveat. This will vary depending on the subject area, context and in some cases, any statutory or regulatory requirements; however, to facilitate information sharing across organisations a consistent approach should be adopted.

Can I use a descriptor to identify information or data that contains personal information?

Only in very specific circumstances to identify certain categories of information that have already been assessed OFFICIAL-SENSITIVE.

The descriptor should be applied in the format: 'OFFICIAL-SENSITIVE [DESCRIPTOR]'

Where descriptors are permitted they must be supported by local policies and business processes and staff training provided.

Can I identify particular processes that involve personal information or data?

If there are business or transactional processes with specific personal information or data related to them, for example a "Court Report" or "Tax Record", then organisations may choose to identify the documents or data in some way to link them to that particular business process and associated handling rules. Such identifiers are not related to the security classification.

Can I send OFFICAL documents containing personal information across the Internet or email them to people on the Internet?

Current rules continue to apply. By default personal information should be protected in transit, i.e. personal information may be sent over the GSi or encrypted across the Internet.

However there are circumstances where it may be appropriate to send unencrypted personal data over the Internet. Before unencrypted personal information is sent across unsecured networks a risk assessment should be undertaken to assess the consequences of compromise. This assessment should also consider the operational or valid business

reasons for this requirement, for example an individual has given permission for their information to be sent via the Internet in order to access or receive a service.

Aggregated datasets of personal information should never be sent unprotected across unsecured networks.

Can personal information be off shored?

Any organisation planning to store or process personal information / data outside the UK/EEA must first consult the Office of the Government SIRO (OGSIRO).

Does OFFICIAL-SENSITIVE personal information have to be registered and tracked?

Where large volumes of OFFICIAL-SENSITIVE personal information or data are regularly shared between organisations, the respective SIROs and IAOs may wish to agree specific handling arrangements and transfer protocols in line with the policy.

How should organisations deal with personal information losses or breaches?

Just as they do now. Organisations must ensure that staff are trained to understand that they have a duty of confidentiality and a personal responsibility to safeguard any HMG information that they are entrusted with. This includes ensuring that they comply with the legal and regulatory requirements and standards, for example the encryption of personal data on removable media.

Incident management policies and procedures should be readily accessible and training supported by common sense local business processes that make it easier for staff to follow the rules (e.g. clear desk policies, guidance on the transmission of personal data, proper disposal, etc). The potential sanctions (criminal or disciplinary) for inappropriate behaviours should be clearly explained to staff and where inappropriate behaviours or security breaches occur they should be dealt with. HR policies and procedures should complement security policies and any disciplinary sanctions should be applied in a measured and proportionate way.

NHS CFA
Data Classification Matrix

		PUBLIC	OFFICIAL/INTERNAL	OFFICAL SENSITIVE / CONFIDENTIAL
Key	Examples of information / data to be handled	Brochures, News releases, Marketing Materials	Routine correspondence, employee newsletters, internal phone directories, inter-office memoranda, non-person identifiable information, internal policies and procedures	Person identifiable information, financial data, purchasing information, vendor contracts
	The consequences if the information / data is mishandled	None	Unauthorised disclosure would not significantly impact NHS CFA, or any of its stakeholders or employees	Unauthorised disclosure could result in significant adverse impact or penalties to NHS CFA, its stakeholders or employees

Transmission by Spoken Word				
	Conversation / Meetings	No special precautions required	Ensure that you are not overheard	Private setting / lowered voices. Avoid public areas, e.g. elevators, hallways, cafeterias etc.
	Landline Telephones	No special precautions required	Ensure that you are not overheard	Avoid proximity to unauthorised listeners. Speakerphone in secure area
	Mobile telephones (including voice enabled blackberries)	No special precautions required	Ensure that you are not overheard	Use of digital telephones preferred
	Voicemail or answering machines	No special precautions required	Ensure that you are not overheard	Only leave name and contact details

Transmission by Post, Fax or e-mail				
	Mail within the NHS CFA (i.e. between buildings)	No special handling required	No special handling required	Sealed inter-office envelope marked Confidential

	Mail outside of the NHS CFA	No special handling required	2nd class mail. No special handling required	2nd class mail. Marked Private and Confidential with return address on the back. Traceable delivery preferred, e.g. Recorded delivery, special delivery etc. use of a courier if a large quantity
	E-mail within the NHS CFA	No special handling required	No special handling required	Refrain from use of personal data. Use of e-mail discouraged where practical
	E-mail outside of the NHS CFA, including internet, N3 & NHSnet Mail	No special handling required	No special handling required	Use of e-mail containing personal data prohibited unless encrypted or emergency situation. Use of e-mail strongly discouraged. Broadcast to distribution lists is prohibited
	Fax Location	Not to be located in an area accessible to the general public	Not to be located in an area accessible to the general public	Not to be located in an area accessible to the general public
	Use of a Fax Coversheet	Required	Required	Required. Coversheet to be labelled Confidential

	Fax Transmission safeguards	Reasonable care in dialling	Reasonable care in dialling	Telephone before transmission to ensure that recipient is waiting by the fax machine for the transmission. Subsequent telephone call to confirm successful receipt of the transmission

Internet and Intranet		Content to be promoted must be authorised by head of section	Content to be promoted must be authorised by head of section	Must not appear on intranet / internet

Magnetic media (including CDs, DVDs, Memory Sticks and Data Cartridges		No special handling required	No special handling required	Use of personal data prohibited unless encrypted or an emergency situation

Electronic File Transfer		No special handling required	No special handling required	Use of personal data prohibited unless encrypted (e.g. using SFTP, FTPS or secure VPN) or a one-off emergency situation

Web Portals (i.e. NHS CFA web-enabled applications)		No special handling required	No special handling required	Use of personal data prohibited unless encrypted (i.e. using HTTPS)

Print, Film, Fiche, Video, DVD Images				
	Printed Materials	No special precautions required	Store out of sight of non-employees	Store out of sight in a secure area
	Sign-in sheets / Sign-in logs	No special precautions required	Placement out of sight of non-employees	Subsequent signers cannot identify signer
	Monitors / Computer Screens	No special precautions required	Positioned or shielded to prevent viewing by non-employees	Positioned or shielded to prevent viewing by unauthorised parties. Possible measures include physical location in a secure area, positioning of screen, use of password protected screen saver, etc.

Copying Standards		No special precautions required	No special precautions required	Photocopying to be minimised and only when necessary

Storage Standards				
	Print Material	No special precautions required	Reasonable precautions to prevent access by non-employees	Storage in a secure manner (e.g. secure area, lockable enclosure)
	Electronic Documents	No special precautions required	Storage on non-public drives only	Storage on secure drives. Storage on shared drives without password protection for reading is prohibited
	E-mail	No special precautions required	Reasonable precautions to prevent access by non-employees	Storage in a secure manner (e.g. password access or reduce to written form, delete electronic form and store in accordance with storage of printed materials)

Destruction Standards				
	Destruction	No special precautions required	No special precautions required	Destroy in a manner that protects confidentiality
	Location of waste paper bins	No special precautions required	Secure area not accessible to	Secure area not accessible to

			unauthorised persons	unauthorised persons
	Paper Recycling	No special precautions required	No special precautions required	Prohibited, unless by special recycling programme for confidential information
	Magnetic media / diskettes	No special precautions required	Overwrite or low-level reformat	Overwrite or low-level reformat

Physical Security Standards				
	Computers / Work Stations	Password protected screen saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work area	Password protected screen saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work area	Password protected screen saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work area
	Printing documentation	No special precautions required	No special precautions required	Printing of documents minimised and when necessary only. Unattended printing is permitted only if physical access are used to prevent unauthorised persons from viewing the

				material being printed
	Office access	No special precautions required	No special precautions required	Access to areas containing sensitive information should be physically restricted. Sensitive information must be locked when left in an unattended room
	Laptops, Smartphones, Blackberries etc.	Password protected screen saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work area. Also laptops must be secured using a locking device when outside of the office environment	Password protected screen saver to be used when briefly unattended. Sign-off or power-off work stations or terminals when not in use or leaving work area. Also laptops must be secured using a locking device when outside of the office environment	Computers must not be left unattended at any time unless the confidential information is encrypted

Access Control		Available to the general public	Generally available to all staff on a need to know basis	Must have a business need to know the information. Must have written approval of the data owner

Audit		None	None	Access should be audited as determined by the data owner