NHS North Yorkshire and York

Title:	**INFORMATION SECURITY POLICY**
Reference No:	NHSNYYIG - 001
Owner:	Director of Standards
Author:	Information Governance Team
First Issued On:	March 2009
Latest Issue Date:	February 2012
Operational Date:	February 2012
Review Date:	April 2013
Consultation Process:	Information Governance Steering Group
Policy Sponsor:	Director of Standards
Ratified and Approved by:	Information Governance Steering Group
Distribution:	All staff
Compliance:	Mandatory for all permanent & temporary employees, contractors, sub-contractors of and those who work jointly with NHS North Yorkshire and York
Equality & Diversity Statement	This policy has been subject to a full equality & diversity impact assessment

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERSION No
05.03.08	Info Gov Mngr	First Draft	0.001
11.02.09	Info Gov Officer	Final Version	1.00
18.08.09	Info Gov Mngr	Update to incorporate further requirements	1.03
25.01.10	Info Gov Team	Update to information security requirements	2.00
December 2011	Info Gov Team	Amended to reflect new organisational structure	2.01

Contents page

1. Introduction

1.1   NHS North Yorkshire and York (NHS NYY) needs robust information security management arrangements for the protection of patient records and key information services, to meet the statutory requirements set out within the Data Protection Act 1998, Caldicott Guidelines, the NHS Confidentiality: Code of Practice and to satisfy their obligations under the Civil Contingencies Act 2004. These aims are also consistent with the UK Strategy for Information Assurance published by the Cabinet Office.

1.2   Without effective security, NHS NYY information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties. NHS NYY and those with whom it contracts and those who supply or make use of NHS NYY information have an obligation to ensure that there is adequate provision for the security management of the information resources that they own, control or use.

1.3   This policy should be read in conjunction with the references listed at the end of this policy.

2 Scope

2.1.   This policy applies to all employees of NHS NYY in all locations including the Non-Executive Directors, temporary employees, locums, contracted staff and volunteers and with those who the NHS NYY contracts with to process information on their behalf.

3 Responsibilities

3.1   **Chief Executive.** The Chief Executive has overall responsibility to ensure that the NHS NYY complies with all legal obligations, relevant legislation, standards and guidelines.

3.2   **Director of** Standards Is the NHS NYY nominated Senior Information Risk Officer (SIRO) and therefore is the designated member of staff who has lead responsibility for information risk within the organisation.

3.3   **Directors, Senior and Line Managers.** Are responsible for ensuring that all staff are aware of and understand their obligations and duties in line with this policy.

3.4   **Information Governance Manager.** Will support the SIRO and Information Asset Owners in the implementation of appropriate Information security controls. In addition will assist and advise on information security incidents investigation and report all such incidents to the Information Governance Steering Group.

3.5   **Information Asset Owners (IAO).** An IAO are senior members of staff who are nominated owners for one of more information assets of the organisation. They must understand the overall business goals of the organisation and how their information assets contribute to or affect these goals. IAOs will document understand and monitor
      3.5.1 What information assets are held and for what purposes
      3.5.2 How information is created amended or added to over time
      3.5.3 Who has access to the information and why

3.6   **NHS NYY Employees**. Employees are responsible for:

3.6.1   The security of information that they create or use in the performance of their duties.

3.6.2   Reporting any suspected or known breaches of information security, or identify weaknesses within information systems they may use, to the Information Governance Manager.
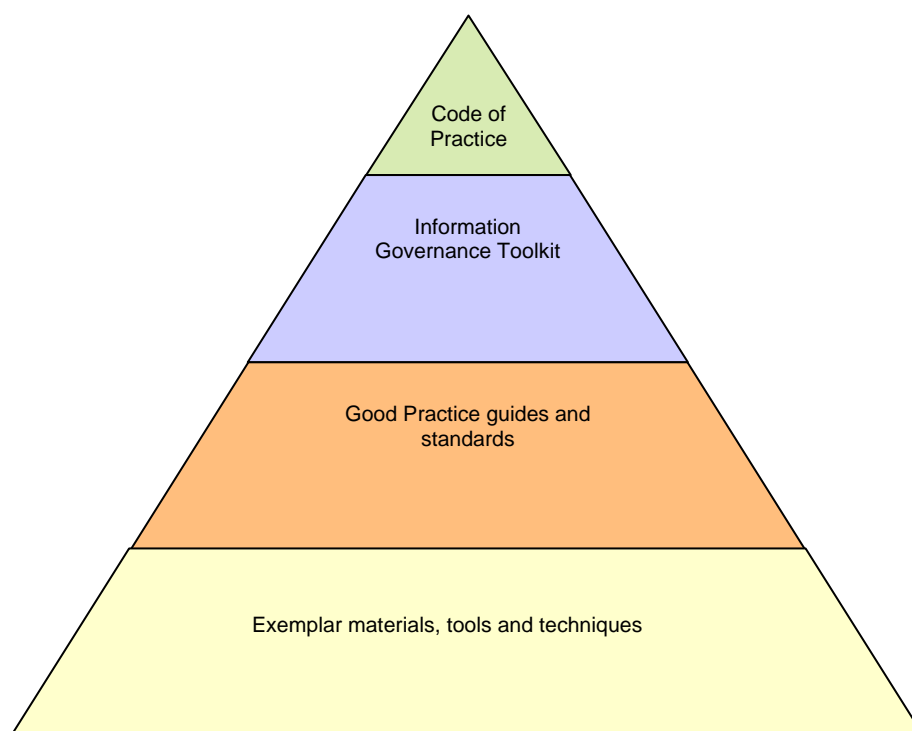
4   Purpose

4.1   The purpose of the Information Security Policy is to protect, to a consistently high standard, all information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external deliberate or accidental through compliance with !S027001.

5   Application of Information Security

5.1   General guidance for all persons listed in the scope of this policy is contained in the Information Security Management : NHS Code of Practice (as may be updated) which is available on the NHS NYY Intranet at:

http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm

Code of Practice

Information Governance Toolkit

Good Practice guides and standards

Exemplar materials, tools and techniques

The NHS Information Security Management Framework

5.2 High quality information underpins the delivery of high quality evidence-based healthcare and many other key service deliverables. Information has greatest value when it is accurate, up to date and is accessible where and when it is needed. Inaccurate, outdated or inaccessible information that is the result of one or more information security weaknesses can quickly disrupt or devalue mission critical processes, and these factors should be fully considered when commissioning, designing or implementing new systems.

An effective information security management system, therefore, ensures that information is properly protected and is reliably available.

5.3   Specific guidance to support these requirements will be written and maintained as part of operational procedures.

6   Security Markings to support Information Governance

6.1   Implementation of an organisational security marking system:

- Allows information to be recognised as a corporate asset and which may be subject to legal obligations and must therefore be handled appropriately.
- Requires that all employees are responsible for the determining the sensitivity and therefore the level of security to be assigned, in accordance with the IAO's requirements
- Provides clear information handling standards which are to be implemented as part of operational procedures for storage, transportation, and destruction in line with minimum information security measures (Annex A)
- Can assist in identifying inappropriate handling of information (Personal identifiable information or corporately sensitive information being left in public areas)

6.2   Security Markings are made up of 3 elements

- Protective Markings, indicate the level of protection that should be given to the information asset.
- Descriptors, words or phrases taken from a limited list that provides an indication of the information content and why the asset has been assigned a protective marker.
- Restrictive Marking indicates how the documents should be handled or distributed.
(See Annex B)

7   Training and Awareness

7.1   Information Governance training is required for all staff and is included as part of the induction and statutory and mandatory training.
7.2   Staff will be made aware of this policy via line management.
7.3   This policy will be available to all staff via the NHS NYY Intranet.

8   Equality and Diversity

8.1   NHS NYY recognises the diversity of the local community and those in its employ. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. All policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

9   Freedom of Information Act 2000

9.1   Any recorded information which is held by, or on behalf of, NHS NYY may be subject to disclosure under the Freedom of Information Act 2000 and Environmental Information Regulations.

10   Records Management

10.1   Records provide evidence and information about the business activities of the PCT and are corporate assets of the NHS NYY. This policy should therefore be retained in line with the NHS Code of Practice on Records Management (Department of Health, 2006). Compliance with this code will ensure that the NHS NYY's records are complete, accurate and provide evidence of and information about the NHS NYY's activities for as long as is required.

11   Review

11.1   This policy will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

12   Monitoring

12.1   Breaches in Information Security will be reported via the NHS NYY's incident reporting mechanisms and will be subject to investigation and reported to the Information Governance Steering Group
12.2   The Audit Commission regularly conducts studies into information security management.
12.3   The NHS Litigation Authority also assesses risk management arrangements through its NHSLA/CNST standards.

13   Discipline

13.1   Breaches of this policy may be investigated and result in the matter being treated as a disciplinary offence under the NHS NYY's disciplinary procedure.

References
NHS Code of Practice: Information Security Management
NHS NYY Confidentiality Policy
NHS NYY Records Management Policy
Data Protection Act 1998
UK Strategy for Information Assurance published by the Cabinet Office

NHS NYY - MINIMUM INFORMATION SECURITY MEASURES

1. **Introduction**. All NHS NYY staff have a duty of confidentiality; this responsibility is included in professional ethics and employment contracts. NHS NYY has a responsibility to ensure adequate information security measures are in place to support and advise individual members of staff to assist them in complying with the corporate legal responsibilities of the NHS NYY.

2. **Background**. Following the loss of 25 million names of child benefit recipients in November 2007 by DWP and the subsequent loss of patient and staff data by other Public Authorities (including NHS organisations), the NHS Chief Executive requested an audit of information and information flows to be carried out by all NHS organisations. This audit is now an annual requirement.

3. The loss of personal information will result in adverse incident reports which will not only affect the reputation of the NHS NYY and NHS Care Records Service but in the case of disclosing personal information intentionally or recklessly is also a criminal offence and fines of up to £500,000 can be imposed by the Information Commissioner on organisations that do not take reasonable steps to avoid the most serious breaches of the Data Protection Act.

4. **Intended Audience**. The measures shown here are intended for all employees. Employees must ensure that information handling in their area of responsibility conforms to the PCT approved standard. All managers must ensure staff have confidence that their handling of information complies with their individual duty of confidentiality.

5. **Purpose**. The aim of the Minimum Information Security Measures in the attached table is to ensure an adequate level of information security assurance is available and adopted throughout the NHS NYY. These measures show Board commitment to support staff and uphold the confidentiality of all sensitive data (i.e. patient, public, staff and corporate). Implementation of, and compliance with these measures is the responsibility of all employees. Advice and support will be given by the NHS NYY's Information Governance Team. These measures will be available for reference on the PCT intranet and will be included as part of the NHS NYY Information Security Framework.

6. **Minimum Measures**. Information is an asset that, depending upon its importance and sensitivity, must be protected appropriately at all times. The measures detailed in the table below are MINIMUM security measures that apply to all NHS NYY information.

7. **Variations to These Measures.**

   7.1. **Increased Measures.** Local variations to increase the level of protection may be applied where necessary (i.e. local risk management has identified the perceived threat is greater than 'normal').

   7.2. **Decreased Measures.** Should there be a local decision to employ measures which do not reach those shown here, then the decision must be approved by the appropriate Information Asset Owner. If the measures are NOT achievable (e.g. due to staffing, training, building space), then this must be treated

as a risk to the NHS NYY and included in the Directorate/Department risk register to ensure the NHS NYY Board is informed.

7.3. **Extreme Situations.** There may be occasions when, due to extreme emergency e.g. patient safety, that the minimum measures cannot be fully applied. In such cases staff should seek approval from an appropriate senior member of staff (if available). The assessment must consider the urgency, information sensitivity (or equipment value), costs involved and other options available. Staff must record any decisions made and the reasons and justification for their decision.

8. **Minimum Scope of Protected Personal Data.** DH have determined that personal data held by the NHS NYY or its Independent Contractors requires protection if the release or loss of the information could cause harm or distress to an individual. This includes all data falling into one or both categories below:

a. **Category A – Identification Data Linked to Sensitive Personal Data**. Information that links an identifiable living person with information about them the release of which would put them at significant risk of harm or distress. This is shown in the table:

Serial	Factual personal information which could be used with public domain information to identify an individual	… combined with	information about that individual whose release is likely to cause harm or distress
	(a)	(b)	(c)
1.	Name / addresses (home or business) / postcode / email / tel numbers / driving licence number / date of birth. [Driving licence number is included as it directly yields date of birth and first part of surname]		Sensitive personal data as defined by s2 of the Data Protection Act, including records relating to the criminal justice system, and group membership e.g.: DNA or finger prints / bank, financial or credit card details / mother's maiden name / National Insurance number / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing

b. **Category B - Identification Data about 1000 Individuals (Or Fewer If Related To High Risk Information or Individuals).** Information about 1000 or more identifiable individuals (other than public domain information) e.g.:

(1) Database with 1000 or more entries containing factual information such as mentioned in 1(a) above.

(2) Electronic folder or drive with 1000 or more records about individuals.

(3) Information on smaller numbers of individuals may also need protection because of the nature of the individuals, nature, source or extent of information.

9. **Colour Codes.** The NHS NYY will use colour codes to help staff identify which level of sensitivity applies to the information content (not format). It may not be necessary to mark each piece of information of low sensitivity or if high volume would make this impractical, however, the colour could be applied to the information 'containers' e.g. file

covers. The mandatory use of coloured markings apply to information classified as High Sensitivity colour code purple.

10.   **Further Development.** These measures will be reviewed frequently. Comments and suggestions are welcome – please send information.governance@nyypct.nhs.uk. Suggestions will be highlighted to the Information Governance Steering Group for consideration.

11.   **Assurance.** The PCT will conduct an information audit annually.

12.   **Glossary of Terms.** Annex A.

MINIMUM SECURITY MEASURES MATRIX

PART ONE – DEFINITIONS AND EXAMPLES

Serial	SUBJECT	PUBLIC INFORMATION	LOW SENSITIVITY	MEDIUM SENSITIVITY	HIGH SENSITIVITY	COMMENTS
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1.	Definitions	Information or material created for the Public Domain or prepared for general disclosure	Information or material (if compromised) that would cause or be likely to cause: • Distress or damage to an individual (patient, staff member, service user, public) • minor damage to operational efficiency of PCT	Information or material (if compromised) that would cause or be likely to cause: • PCT financial loss or loss of earning potential • facilitate improper gain or advantage • prejudice investigation or facilitate crime • breach confidentiality owed to 3rd parties • impede development or operation of PCT policies • breach statutory restrictions on disclosure • disadvantage PCT negotiations • undermine public sector management • significant or substantial distress or damage caused to an individual (patient, staff member, service user, public)	Information or material (if compromised) that would cause or be likely to cause, prejudice, seriously impede or substantially undermine: • individual security • financial viability (Public Authority) • work of the NHS • Govt policy • serious crime investigation (or facilitate serious crime)	
2.	Examples	**Information examples**: PCT addresses information, job adverts, annual reports, publicity material, brochures, advice leaflets - Public record documents and website information, publicising PCT services, anonymised statistics, public appointments, information disclosed following an FOI request, e-mail address of senior managers or customer facing staff **Equipment examples**: N/A	**Information examples:** Routine letter to patient, internal communications, internal policies and procedures, general business documents, phone directories, employee publications, Organisation plans, internal operational information. **Equipment examples**: value less than £500 including: CfH Smartcards, Printers, small processing applications,	**Information examples**: patient health record, employee information, particularly sensitive identifiable patient letters e.g. communicable diseases, transaction documents and reports, technical information, security information, e-mail lists of all non senior staff, service redesign information (prior to publication), **Equipment examples:** value less than £1000 including: Encrypted Laptop, Encrypted PDA, Encrypted Memory Sticks, Encrypted blackberries, Cameras, Directorate systems, Service processing systems	**Information examples**: details of individuals at high risk of personal attack, bulk lists of basic personal data, serious security weaknesses, details of audit / financial / governance systems, particularly sensitive case notes or person identifiable information **Equipment examples:** of value greater than £1000 including: computer, servers, corporate processing systems	
	Aggregating Sensitivity	Large amounts of public information (e.g. leaflets) have no	More than 20 LOW sensitivity records must be handled as if MEDIUM ➔➔	More than 20 MEDIUM sensitivity records must be handled as if HIGH ➔➔		

		greater sensitivity than a single public document				

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
1.	CREATE & PROCESS INFORMATION					
1.1.	Information Asset Owner identified	Required	Mandatory	Mandatory	Mandatory	Responsibilities included in Job Description
1.2.	Authority to create / obtain / receive / retrieve / transfer	Any member of staff	Staff who process Information Asset	Authorised by Information Asset Owner (IAO)	Authorised by Information Asset Owner	IAO must authorise all information collections and uses
2.	SHARING / DISCLOSING					
2.1.	Authority to share / disclose	Any member of staff	Information Asset Owner, Health Professional, or those acting on behalf of.	Information Asset Owner, Service Managers, Consultants, RMO's, Key Workers or those acting on their behalf.	Senior Managers, Heads of Service, Asst Directors, Consultants, RMO's or those authorised by the above	IAO must authorise all information Sharing and disclosure Info Sharing Protocol for **routine** sharing of AMBER and above if not for direct healthcare
3.	EDUCATION, AWARENESS AND TRAINING					
3.1.	Mandatory Annual Training	All staff	All staff	All staff	All staff	
4.	INCIDENT REPORTING					
4.1.	Suspected or potential incident via PCT Reporting System	Good Practice (within 24 hrs of incident occurring)	Mandatory (within 24 of incident occurring) SUI's ASAP	Mandatory (within 24 hrs of incident occurring)- SUI's ASAP	Mandatory immediate (ASAP – within 24hrs of incident occurring) SUI's ASAP	These will be dealt with under the PCT Incident Reporting Policy (loss of properly encrypted media is not a SUI).
4.2.	Highlight potential weakness and / or 'near miss'	Good Practice (within 24 hrs of incident occurring)	Mandatory (within 24 of incident occurring)	Mandatory (within 24 hrs of incident occurring)	Mandatory immediate (ASAP – within 24hrs of incident occurring)	
4.3.	Audit Trails and Access	Not Required	Mandatory where possible	Mandatory where possible	Mandatory where possible	Information

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

Serial (a)	PROCESS (b)	GREEN (c)	AMBER (d)	RED (e)	PURPLE (f)	NOTES (g)
	Monitoring					Asset Owner to ensure
5.	DOCUMENTED GUIDANCE					
5.1.	Written procedures available to Staff	Not required	Mandatory	Mandatory	Mandatory	Verbal guidance is always to be given
5.2.	Procedures Training / Assurance to Staff	Not required	Mandatory	Mandatory	Mandatory	
5.3.	Regular audit of procedure compliance	Not required	Mandatory	Mandatory	Mandatory	Information Asset Owner to ensure
6.	SECURITY MARKINGS					
6.1.	Protective Marking[1]					
6.1.1.	Hardcopy information	Blank OR Good Practice 'Protective Marking – GREEN'	Blank OR Good Practice 'Protective Marking – AMBER'	Mandatory 'Protective Marking – RED'	Mandatory 'Protective Marking – PURPLE'	See also 'Authority to create'
6.1.2.	Unencrypted electronic data media, CDs/DVDs, CCTV, tape recording, unencrypted memory stick	Not allowed- so not applicable	Not allowed - so not applicable	Not allowed – so not applicable	Not allowed – so not applicable	See also 'Authority to create'
6.2.	Descriptor	Not Required	Not Mandatory	Mandatory	Mandatory	
6.3.	Restrictive marking	Not Applicable	Not Mandatory	Mandatory	Mandatory	
7.	STORING – WHERE AND HOW TO STORE					
7.1.	Hardcopy documents	Non public areas unless for display	Protected by lockable door from public or shared area and unauthorised access	Lockable container, drawer or a room which is itself protected by lockable door from public (or shared workforce area to prevent unauthorised access)	Secure container protected by 2 lockable doors from public (or shared workforce area) to prevent form unauthorised access.	Applies when work area is unoccupied
7.2.	Electronic information	Common Shared Directories on NHS Network, encrypted laptop or memory	Access Controlled Directory or Individual Access on NHS	Access Controlled Directory or Individual Access on NHS		Personal information must

---

[1] Document templates are on the intranet - http://nww.nyypct.nhs.uk/Corporate/DocTemplates/index.htm

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
		sticks (all laptops are now encrypted)	Network. Temporary authorised storage on encrypted laptop or encrypted memory sticks, information to be securely transferred to NHS Network ASAP & removed from temporary encrypted laptop or memory stick immediately following transfer.	Network. Temporary authorised storage on encrypted laptop or encrypted memory sticks, information to be securely transferred to NHS Network ASAP & removed from temporary encrypted laptop or memory stick immediately following transfer.	Access Controlled Directory or Individual Access on NHS Network with file password protection.	never be stored on CD, DVD, or any unencrypted removable or any portable devise or non authorised equipment.
7.3.	Storage of authorised Encrypted Memory stick, (all are password protected)	Protected by lockable door from public (or shared workforce area	Protected by lockable door from public (or shared workforce area)	Protected by lockable door from public (or shared workforce area)	Protected by lockable door from public (or shared workforce area)	Only authorised equipment maybe used
7.4.	Personal Computers	Allowed	Not Allowed	Not Allowed	Not Allowed	
7.5.	PCT Mobile Phone - Unencrypted	Allowed (Access protected by PIN to prevent misuse)	Not Allowed	Not Allowed	Not Allowed	
7.6.	PCT Mobile Phone - Encrypted	Allowed (Access protected by PIN to prevent misuse)	Not Allowed	Not Allowed	Not Allowed	
7.7.	Personal Mobile Phone - Unencrypted	Not Allowed	Not Allowed	Not Allowed	Not Allowed	
8.	ENCRYPTION[2]					
8.1.	Device Encryption (e.g. laptop, Blackberries	Organisationally Authorised Encryption	Organisationally Authorised Encryption	Organisationally Authorised Encryption	Organisationally Authorised Encryption	Only authorised equipment maybe used
8.2.	Device Encryption removable media memory sticks,	Organisationally Authorised Encryption	Organisationally Authorised Encryption	Organisationally Authorised Encryption	Organisationally Authorised Encryption	Only authorised equipment maybe used
8.3.	End Point Control (for PCT networks)	Authorised End Point Control	Authorised End Point Control	Authorised End Point Control	Authorised End Point Control	
9.	ROUTINE TRANSPORTING / TRANSMISSION					
9.1.	Post					

[2] If exceptional situations apply e.g. data cannot be encrypted for legal or business reasons (uncertainty of speed or accurate recovery) then other measures must be in place to ensure the data is adequately protected using strong controls e.g. recorded, moved, stored and monitored.

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED						
Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
9.2.	Post (Hard copy info)[3]	First or Second Class	First Class or Second Class	Recorded Signed	Special Delivery tracked	
9.3.	Post (Electronic encrypted data)	First or Second Class	First Class or Second Class	Secure electronic transfer whenever possible or where authorised Recorded signed	Secure electronic transfer whenever possible or where authorised Special Delivery tracked	
9.4.	Post (Electronic **Non** encrypted data)	First or Second Class	*Not allowed	*Not allowed	*Not allowed	*Unless agreed by the Board following a full Risk Assessment
9.5.	**Packaging**					
9.6.	Post	Adequate for content size and weight	Robust single wrapper (e.g. tamper proof pouch, envelope) to individuals	• Sent to organisations - double wrapper (e.g. outer wrapper of tamper proof pouch, envelope) • Sent to individuals (e.g. patient) – robust double envelope	Double wrapper (e.g. lockable, pouch, envelope)	Implement tracking in line with records management policy
9.7.	NHS and Non – NHS Courier	Adequate for content size and weight	Robust single wrapper (e.g. tamper proof pouch, envelope)	Sent to organisations - double wrapper (e.g. outer wrapper of tamper proof pouch, envelope)	Double wrapper (e.g. lockable, pouch, envelope)	Implement tracking in line with records management policy
9.8.	PCT Staff Possession	Adequate for content size and weight	Locked container	Locked Container	Locked Container	Implement tracking in line with records management policy
9.9.	**Address details**	Ensure correct address	Ensure correct address and return to sender address(not NHS	• Organisations - outer envelope addressed to	Outer envelope addressed to organisation.	

[3] First Class delivered in 1 to days, Second Class delivered in 3+ days, Recorded Signed for (fee plus normal postage, gives proof of posting and an electronic copy of the signature on delivery). Special Delivery 9.00am tracked from despatch to delivery and an electronic copy of the signature. Special Delivery Next Day tracked from despatch to delivery and an electronic copy of the signature. Safebox for sending and receiving diagnostic specimens.

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
			identifiable (for patient letters)	organisation, inner envelope marked 'exclusive for' the person's appointment • Patients - outer envelope addressed to patient, inner envelope marked 'exclusive for' the person's appointment	Inner envelope marked 'exclusive for' the person's appointment	
9.10.	Fax					
9.10.1.	Fax - sending	No Restriction	Use a confirmed number in working hours only OR treat as RED	Confirm identity and that individual is an authorised recipient, and location and from and to a confirmed Safe Haven[4]	Not allowed	Cover sheet ALWAYS showing Safe Haven Fax no:
9.11.	Telephones	No Restriction	Confirm identity and that individual is an authorised recipient	Confirm identity and that individual is an authorised recipient, and location	Not allowed	
10.	Courier					
10.1.	Courier (hard copy info)	Member of PCT Staff or Non NHS Courier or NHS Courier Transport	Member of PCT Staff or Non NHS Courier or NHS Courier Transport	Authorised and named member of PCT staff OR Non NHS Courier or NHS Courier Transport	Authorised and named member of PCT staff or Non NHS Courier or NHS Courier Transport	Implement tracking in line with records management policy
10.2.	Courier (Electronic encrypted data)	Member of PCT Staff o Non NHS Courier or NHS Courier Transport	Member of PCT Staff or Non NHS Courier or NHS Courier Transport	Secure electronic transfer whenever possible. Authorised and named member of PCT Staff or Non NHS Courier or NHS Courier Transport	Secure electronic transfer whenever possible Authorised and named member of PCT staff OR Non NHS Courier or NHS Courier Transport	Implement tracking in line with records management policy
10.3.	Courier (Electronic **Non** encrypted data)	Member of PCT Staff or Non NHS Courier or NHS Courier Transport	Not Allowed	Named member of PCT staff - **not allowed unless essential for patient care** Non NHS Courier* - **not allowed unless essential for patient**	Named member of PCT staff - **not allowed unless essential for patient care** Non NHS Courier* - **not allowed unless essential for patient**	*Notify to PCT Board (DH Directive Dec 07) following a Risk Assessment

---

[4] Safe Haven guidance on PCT intranet at: Section 5: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
				care NHS Courier Transport* - **not allowed unless essential for patient care**	care NHS Courier Transport* - **not allowed unless essential for patient care**	record reasons for transportation
11.	Individual Staff					
11.1.	Authority to remove from NHS location	No Restriction	As approved by IAOs	As approved by IAOs	As approved by IAOs	
11.2.	Authority to Transport between business locations	No Restriction	As approved by IAOs	As approved by IAOs	As approved by IAOs	
11.3.	From secure business premises using secure PCT remote access	Allowed	Allowed	Allowed	Allowed	Only when approved by IAOs and using authorised secure mechanisms
12.	REMOTE WORKING					
12.1.	From home using secure PCT remote access	Allowed	Allowed	Allowed	Not Allowed	Only when approved by IAOs and using authorised secure mechanisms
12.2.	Working at Home (occasional)	Line Manager	As approved by IAOs	As approved by IAOs	Not Allowed	Only when approved by IAOs and using authorised secure mechanisms
12.3.	Working from Home (long term/frequent)	Awaiting home working policy	Awaiting home working policy	Awaiting home working policy	Not allowed	All levels need HR authorisation
13.	E-Mail					

Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
13.1.	[5] from nhs.uk to nhs.uk	Allowed	Not Allowed	Not Allowed	Not allowed	E-mail systems with addresses such as @nyypct.nhs.uk @acute.sney.nhs.uk @york.nhs.uk @hdft.nhs.uk etc
13.2.	[6] from nhsmail to nhsmail	Allowed	When appropriately authorised Allowed • No Patient Identifiable Data in subject heading. • Password protect file. • Include disclaimer.	When appropriately authorised Allowed • No Patient Identifiable Data in subject heading. • Password protect file. • Get delivery receipt. • Include disclaimer.	When appropriately authorised Allowed • No Patient Identifiable Data in subject heading. • Password protect file. • Get delivery receipt. • Include disclaimer.	This is available to all NHS staff – most often seen as 'xx@nhs.net'
13.3.	from nhsMail to secure govt e-mail addresses	Allowed	When appropriately authorised Allowed • No Patient Identifiable Data in subject heading. • Password protect file. • Include disclaimer.	When appropriately authorised Allowed • No Patient Identifiable Data in subject heading. • Password protect file. • Get delivery receipt. • Include disclaimer.	When appropriately authorised Allowed • No Patient Identifiable Data in subject heading. • Password protect file. • Get delivery receipt. • Include disclaimer.	Govt secure addresses: **gsi**.gov.uk; **gsx**.gov.uk; **gse**.gov.uk; scn.gov.uk; pnn.police.uk; cjsm.net; Nhs.net x.gsi.gov.uk police.uk
13.4.	to govt and official mail addresses	Allowed	Not Allowed	Not Allowed	Not allowed	e.g. gov.uk
13.5.	to smtp (e.g. yahoo, hotmail)	Allowed in response to patient / public's. Include disclaimer.	Not Allowed	Not Allowed	Not allowed	

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

[5] NHSMail or other encryption approved by the Head of IM&T to be used wherever and whenever possible. For patient safety and business critical communications the Interim Measures are allowed until NHSMail or equivalent is in place. Register for NHSMail at: https://www.nhs.net/

[6] Please note you must send FROM an NHS mail account TO an NHSMail account for the message to be secure. Sending from 'nyypct.nhs.uk to @nhs.net is NOT secure.

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED

Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
14.	PRINTING					
14.1.	Printing to	Any printer	Networked supervised	Dedicated, non-shared	Dedicated, non-shared in office restricted to Information Asset staff (Safe Haven)	
15.	SECURE DESTRUCTION					
15.1.	Authority to destroy	Any appropriate member of staff	Information Asset Staff	Information Asset Staff	Manager of Information Asset, Service Managers	Retention Schedules at listed in the [7]Records Management CoP
15.2.	Paper	Tear into large pieces or mark to show it has been checked – throw away with normal rubbish or **recycle**	Small quantities - shred on site and dispose of with larger quantity of GREEN paper waste. Larger quantities aggregate to RED	Cross cut shredder or secure Contractor services	Cross cut shredder or secure Contractor services	
15.3.	Floppy Disks	Not Allowed	Storage on these devices not allowed	Storage on these devices not allowed	Storage on these devices not allowed	
15.4.	CD / DVDs	mark or break to show it has been checked – throw away with normal rubbish or **recycle**	Storage on these devices not allowed	Storage on these devices not allowed	Storage on these devices not allowed	
15.5.	Computer Disks (Hard drives)	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	
15.6.	Memory Stick (encrypted)	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.	
15.7.						

---

[7] Records Management Code of Practice available at: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/PoliciesGuidelines.htm

PART 2 – THE THINGS WE DO WITH INFORMATION AND MINIMUM MEASURES TO BE USED						
Serial	PROCESS	GREEN	AMBER	RED	PURPLE	NOTES
(a)	(b)	(c)	(d)	(e)	(f)	(g)
	NON ENCRYPTED MEMORY STICKS, LAPTOPS, PALMTOPS AND PDAs MUST NOT BE USED					

Guide to Security Markings

Protective markings entered into the FOOTER of documents					
Protective Marking	**Definitions and examples**	**Descriptor**	**Definitions and examples**	**Disposal of Manual Records (in line with Records Management Policy)**	**Disposal of Electronic Records (in line with Records Management Policy)**
GREEN	Public record documents, PCT address information, job adverts, annual reports, publicity material, brochures, advice leaflets - website information	N/A	Nil	GREEN documents can be recycled; does not need secure destruction or additional markings	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.
AMBER	Internal communications, internal policies and procedures, general business documents, phone directories, employee publications, routine letter to patient *Non - sensitive personal/patient data (minor distress)* - intranet site information, internal operational information.	**Commercial**	Relating to a commercial undertaking's processes or affairs.	Small quantities - shred on site and dispose of with larger quantity of GREEN paper waste. Larger quantities aggregate to RED	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.
		Contracts	Concerning tenders under consideration and the terms of tenders accepted.		
		Draft	Information for review, amendment & approval (content and accuracy) within 1 month.		
		Management	Concerning policy or planning affecting the interests of staff.		
RED	Patient health record, Employee information, transaction documents and reports, technical information, security information, *sensitive personal/patient data (significant or substantial distress).*	**Medical**	Medical reports and records, and material relating to them.	Cross cut shredder or secure Contractor services	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.
		Patient	References to named or identifiable patients.		
		Personal	Material only to be seen by the person to whom it is addressed.		
PURPLE	Information likely to prejudice, or substantially undermine individual security, financial viability, work of the NHS, govt policy, serious crime investigation (or facilitate such) details of individuals at high risk of personal attack, bulk lists of basic personal data, serious security weaknesses, details of audit / financial / governance systems, particularly sensitive person identifiable information	**Private**	Information collected/ sent through NHS electronic services where access needs to be limited to appropriate official(s).	Cross cut shredder or secure Contractor services	Delete all data (including from the recycle bin if applicable) and pass securely to IT Dept with your details and mark item requires secure destruction of data.
		Prohibited	Information prohibited from disclosure by legislation or enactment or the information is (or may become) the subject of, or concerned in legal action or investigation		
		Publication	Information intended for publication within 2 - 3 months.		

All Markings must be applied by the originator. Protective Markings are decided according to the information content and by the Information Asset Owner. Restrictive Markings are decided in accordance with how the document should be handled or distributed

Restrictive Markings in HEADER	
Restrictive Marking	**Definition**
Not for further disclosure	Not to be sent on to a third party
Not for further disclosure without reference to the originator	Not to be sent on to a third party without the originators permission
GUM Staff only	Limited to GUM staff
PCT Internal use only	Not for distribution outside the PCT
Restricted distribution e.g. Board, Directors and Heads of Service Only	Circulation restricted to those shown

GLOSSARY OF TERMS

Serial	Term	Meaning	Explanation/Comment
1.	Personal Information	Information that alone or together with other information held by or obtainable by the organisation can identify an individual	
2.	Sensitive Information	Information consisting of racial or ethnic origin, political opinions, religious or other beliefs, whether the individual is a member of a trade union, physical or mental health condition, sexual life, the commission or alleged commission of an offence, or any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.	
3.	Corporate Information	Information relating to the organisation and how it fulfils its functions, for example contracts with suppliers, minutes of meetings, financial information.	
4.	Information Asset	An information asset is a collection of information e.g. files such as personnel records; a database of information such as PCT staff issued with mobile phones; the master minutes of PCT meetings.	
5.	Senior Information Asset Owner (SIRO)	Will be either the Executive Director or Senior Management Board Member who takes overall ownership of information risk and acts as champion for information risk on the Board. The SIRO will • Understand how the strategic business goals of the organisation and how other NHS organisations business goals may be impacted by information risks and how these risks may be managed • The SIRO will implement and lead the IG risk assessment and management processes within the organisation and advise the Board on the effectiveness of information risk management across the organisation	

6.	Information Asset Owners (IAO)	Are Senior members of staff who are nominated owners for one of more information assets of the organisation and must understand the overall business goals of the organisation and how their information assets contribute or affect these goals. IAOs will document understand and monitor • What information assets are held and for what purposes • How information is created amended or added to over time • Who has access to the information and why	
7.	Information Asset Administrator	Information Asset Administrators can be delegated with responsibilities from Information Asset Owners	
8.	Information Processing / Handling	This means obtaining, recording or holding information or carrying out any operation or set of operations on that information including: • Organisation, adaptation or alteration of that information, • Retrieval, consultation or use of the information, • Disclosure of the information by transmission, dissemination, or otherwise making it available, • Alignment, combination, blocking, erasure or destruction of the information.	
9.	Information (Data) Subject	Means an individual who to whom the information relates.	

Information Governance Reporting Structure

```
                                    ┌─────────────────┐
                                    │   PCT Board     │
                                    └─────────────────┘
        ┌──────────────────┐
        │     Audit        │
        │   Committee      │
        └──────────────────┘
                                    ┌─────────────────┐
                                    │   Governance    │
                                    │   and Quality   │
                                    │   Committee     │
                                    └─────────────────┘

   ⬭ CHECK                                                        ACT ⬭

                                    ┌─────────────────┐
                                    │   Information   │
                                    │   Governance    │
                                    │  Steering Group │
                                    └─────────────────┘

  ┌────────────┐   ┌─────────────┐  ┌────────────┐   ┌────────────┐
  │Information │   │Information  │  │Data        │   │Records     │
  │Governance │   │Security     │  │Protection  │   │Management  │
  │Management │   │Management   │  │and FOI     │   │and Data    │
  │Group      │   │Forum        │  │Working     │   │Quality     │
  └────────────┘   └─────────────┘  │Group       │   └────────────┘
                                    └────────────┘

  ⬭ DO        ┌────────────┐    ┌─────────────┐        PLAN ⬭
              │Registration│    │Secondary Use│
              │Authority   │    │Assurance    │
              │Working     │    │Working Group│
              │Group       │    └─────────────┘
              └────────────┘
```

| Guidance and Regulation | ──────────► |
| Risks Identified | – – – – –► |