Stockport NHS
NHS Foundation Trust

Information Classification Policy

State whether the document is: ☑**Trust wide**	**State Document Type:** ☑ **Policy**
APPROVAL VALIDATION	Information Governance Committee Finance & Performance Committee
DATE OF APPROVAL VALIDATION	19 July 2017 August 2017
INTRODUCTION DATE	August 2017
DISTRIBUTION	Information Governance & Security Microsite
REVIEW	**First Issue Date** April 2011 **Review Date** August 2019
CONSULTATION	Information Security Group
EQUALITY IMPACT ASSESSMENT	☑ **Screening**
RELATED APPROVED TRUST DOCUMENTS AND ASSOCIATED GUIDANCE	Information Governance Policy Information Governance Strategy Information Security Policy Information Security Incident Reporting/Management Information Sharing & Transfer of Records Policy System Level Security Procedure IT Acceptable Use Policy Mobile Devices & Removable Media Security Policy Remote Access & Mobile Working Policy Photography/Video & Audio Records of Patients Network Security Policy Data Protection & Confidentiality Policy Access to Health Records Policy Data Quality Policy Freedom of Information Policy Records Management Policy Records Management Strategy Disciplinary Policy Incident Reporting SOP Government Security Classifications 2014 (*guidance)*
AUTHOR/FURTHER INFORMATION	Khaja Hussain Asst. Director, Information Governance & Security
VERSION NO.	2.1 (July 2017)
THIS DOCUMENT REPLACES	2.0 (April 2016)

Document Change History:			
Issue No	**Page**	**Changes made** (include rationale and impact on practice)	**Date**
2.1	*6,* *10*	*Clarification of classification criteria* *Additional of Classification Summary*	*July 2017*
2.0		*Refreshed / Redrafted Policy to comply with updated Govt. guidance*	*April 2016*
1.0 (Draft)		*New Policy*	*March 2011*

Contents

1. Introduction/Purpose of the Document

The updated Government security classifications came into force on 02 April 2014. These classifications provide guidance on information asset classification to ensure they are appropriately protected, that they support Public Sector business and that they meet the requirements of all relevant legislation. The classifications apply to **all** information that government departments, including the NHS, collects; stores; processes; generates or shares to deliver services and conduct its business. It also includes information received from or exchanged with 3rd parties.

All employees have a duty to respect the confidentiality and integrity of the NHS information and data that they access and are personally accountable for safeguarding the Trust's information assets in line with this, and other Information Governance, policies.

Further NHS IG guidance is also available on the Information Governance & Security microsite on the Trust's intranet.

2. Statement of Intent/Scope of the Document

This document describes the classification guidelines for information within the Trust and also the policy for how information assets are to be labelled and handled based on their classification. Information will be controlled in accordance with its 'protective mark' as specified within other Trust documentation.

This document applies to both information recorded on paper and that processed electronically including printouts, reports etc.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement.

3. Summary of the Document

This document sets out a simple scheme of classification relevant to the needs of NHS organisations and for the common benefit of all. It has been formulated according to the Government's simplified security classification, a copy of which is available on the IG & Security Microsite.

The Government's guidance sets only 3 classifications for all information assets – **OFFICIAL**, Secret and Top Secret. In practice, NHS organisations would only use '**OFFICIAL**'; 'Secret' and 'Top Secret' relating to organisations where loss or damage could compromise military capabilities or cause widespread loss of life.

All information within the Trust, whether collected, generated, processed or shared will be classified as **OFFICIAL**, with the addition of descriptors to reinforce the 'Need to Know' requirement.

Classification is essential to ensure that information assets receive the level of protection that is appropriate in terms of their worth to the NHS and applies to information (or other specific

assets) and controls applied to effectively manage associated confidentiality, integrity and available risks – determined on a case by case basis following a robust risk assessment.

4. Definitions

4.1 OFFICIAL

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which will have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

4.2 Secret

Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military operations, international relations or the investigation of serious organised crime.

4.3 Top Secret

HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

5. Roles & Responsibilities

5.1 Corporate Records Management Group:

The Corporate Records Management Group will be responsible for monitoring compliance with this policy and ensuring that the necessary processes are in place to enable the policy to be adhered to in full.

5.2 Information Security Group:

The Information Security Group will be responsible for ensuring that this policy is implemented across all Trust systems.

5.3 All Trust Managers:

Managers within the Trust are responsible for ensuring that the policy, and other associated policies and supporting standards and guidelines are built into local processes and that there is on-going compliance.

Managers are accountable for the communication about and compliance with Trust policies, and must ensure that staff are adequately trained and apply the appropriate guidelines.

Managers should ensure that access to all classified information (i.e. information that is of value to the business / is protectively marked) is restricted consistently with this policy and

that procedures and systems are in place to implement appropriate access controls, to ensure that information is stored and transported securely and is not lost or corrupted.

5.4 All Trust Staff:

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff are responsible for any records or data they create and what they do with information they use.

Staff should ensure they attend information governance training and awareness sessions to maintain their knowledge and skills.

Staff must be trained to understand that they are **personally responsible** for securely handling any information that is entrusted to them in line with local business processes.

Staff should be aware that access to **sensitive** information must **ONLY** be granted on the basis of genuine 'need to know' and an appropriate security control

6. The Policy

All information used by the Trust is, by definition, '**OFFICIAL**.' It is highly unlikely that we will work with 'SECRET' or 'TOP SECRET' information.

Things to remember about **OFFICIAL** information:

6.1 There is no requirement to explicitly mark **routine** **OFFICIAL** information. Ordinarily **OFFICIAL** information does not need to be marked for non-confidential information.

6.2 A limited subset of **OFFICIAL** information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the **OFFICIAL** classification tier, but should have additional measures applied in the form of **OFFICIAL-SENSITIVE**.

6.3 Within the Trust, due to the historic nature of NHS Health Records and Staff Records, which are marked "Confidential" or "NHS Confidential", these should be treated as **Official-Sensitive** documents, as specified in this classification policy.

6.4 How to Handle and Store OFFICIAL Information

EVERYONE is responsible for handling **OFFICIAL** information with care by:

- Apply a clear desk policy
- Only share information with the appropriate people
- Take extra care when sharing information with external partners i.e. sending information to named recipients at known addresses
- Always lock your screen before leaving the computer
- Use discretion when discussing information out of the office

6.5 How Handle and Store OFFICIAL-SENSITIVE Information

All **OFFICIAL-SENSITIVE** material including documents, staff records, Health records on all media (electronic; paper; visual; audio) and other material should be physically secured to prevent unauthorised access.

As a minimum, when not in use, **OFFICIAL-SENSITIVE** material should be stored on a secure, encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

- Always apply appropriate protection and comply with the handling rules (*see Information Sharing & Transfer of Records Policy)*
- Always question whether your information may need stronger protection
- Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains, etc
- Only print **OFFICIAL-SENSITIVE** information when absolutely necessary
- Only send **OFFICIAL-SENSITIVE** information by the secure email route or use encrypted data transfers
- Encrypt all sensitive information stored on removable media particularly where it is outside the organisation's physical control

- Store information securely when not in use and use a locked cabinet/drawer if paper is used

- If faxing the information, make sure the recipient is expecting your fax and double check their fax number
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details

- NEVER send **OFFICIAL-SENSITIVE** information to internet email addresses e.g. Gmail, Hotmail, etc

- Only in exceptional cases, where a business need is identified, should **OFFICIAL-SENSITIVE** information be emailed over the internet, in an encrypted format, to the third parties. Contact the IG team for further advice

- The use of pin code for secure printing is both widely available and preferable way to manage the printing process

7. Implementation

7.1 The responsibility of implementing this document, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff (including agency staff) to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

7.2 This document has been compiled by the Information Governance Team utilising guidance issued by the Cabinet Office. It will be reviewed/monitored as part of the Trust's IG Framework

Once finalised, the document will be presented to the Performance & Finance Committee. The document will then be displayed on the Information Governance & Security microsite on the Trust's intranet and on the Trust's website. Managers and Governance leads should ensure the information is cascaded to all staff.

This Policy will be reviewed biennially or more frequently if appropriate to take into account changes to legislation that may occur, and/or guidance from the Cabinet Office, Department of Health, the NHS Executive and/or the Information Commissioners Office (ICO).

This policy is directly referenced to BS 1008 and any changes to policy need to be checked for compliance.

8. Monitoring

The Trust will regularly monitor and audit its Data Protection practices for compliance with this policy.

The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the policy is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Information Governance Committee, Finance & Performance Committee, Quality Assurance Committee and the Audit Committee, as appropriate.

The Information Commissioner may also mandate an audit upon the Trust at any time.

Monitoring Arrangements	**Responsibility / Process / Frequency**
Process for monitoring e.g. audit	- Internal Audit - Information Governance Toolkit - External Audit
Responsible individual/ group/ committee	Information Governance Committee
Frequency of monitoring	Biennially
Responsible individual/ group/ committee for review of results	Information Governance Committee
Responsible individual/ group/ committee for development of action plan	Information Governance Committee
Responsible individual/ group/ committee for monitoring of action plan	Information Governance Committee

Appendix 1 – ClassificationSummary

Information Classification Summary - Examples

Official	**Official-Sensitive**
Policies	Health Records
Procedures	Staff Records
SOPs	EPR/Clinical Systems
SFT Intranet	Restricted Access Drives where access is limited to specific staff with a defined need for access. E.G. Information could contain personal or business sensitive information
SFT Website	
Open Access Drives for all staff or departmental drives with open access for all staff	

The above is by no means an exhaustive list, but gives you examples as a guide.

Stockport NHS Foundation Trust

Office Use Only

Submission Date:	***July 2016***
Approved By:	***Sue Clark***
Full EIA needed:	**No**

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the Policy/SOP/Service**	Information Classification Policy	
2	**Department/Business Group**	Information Governance/IM&T	
3	**Details of the Person responsible for the EIA**	**Name:**	Jean Lehnert
		Job Title:	I.G. Co-ordinator
		Contact Details:	0161 419 4364
4	**What are the main aims and objectives of the Policy/SOP/Service?**	To provide guidance to staff on the appropriate classification of information in accordance with the Trust's accreditation for NHS Mail.	

For the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a <u>differential</u> impact on any of the protected characteristics? If so, is this impact likely to be positive or negative?** **Consider:** • Does the policy/SOP apply to all or does it exclude individuals with a particular protected characteristic e.g. females, older people etc.? • What does existing evidence show? E.g. consultation from different groups, demographic data, questionnaires, equality monitoring data, analysis of complaints. Are individuals from one particular group accessing the policy /SOP /Service more/less than expected?	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Designate a timescale to monitor the impacts. ✓ Re-visit after the designated time period to check for improvement.	**Lead**
Age	No impact – the policy does not relate to specific characteristics about living individuals		
Carers / People with caring responsibilities	No impact – the policy does not relate to specific characteristics about living individuals		

Disability	No impact – the policy does not relate to specific characteristics about living individuals		
Race / Ethnicity	No impact – the policy does not relate to specific characteristics about living individuals		
Gender	No impact – the policy does not relate to specific characteristics about living individuals		
Gender Reassignment	No impact – the policy does not relate to specific characteristics about living individuals		
Marriage & Civil Partnership	No impact – the policy does not relate to specific characteristics about living individuals		
Pregnancy & Maternity	No impact – the policy does not relate to specific characteristics about living individuals		
Religion & Belief	No impact – the policy does not relate to specific characteristics about living individuals		
Sexual Orientation	No impact – the policy does not relate to specific characteristics about living individuals		
General Comments across all equality strands	The policy seeks to provide guidance to staff to enable them to appropriately classify documents. It does not refer to or relate to any living individuals or their specific characteristics.		

EIA Sign-Off	**Your completed EIA should be sent to Sue Clark , Equality and Diversity Manager for approval and publication:** Susan.clark@stockport.nhs.uk **0161 419 4784**

If you would like this policy in a different format, for example, in large print, or on audiotape, or for people with learning disabilities, please contact:
Patient and Customer Services, Poplar Suite, Stepping Hill Hospital. Tel: 0161 419 5678.
Email: PCS@stockport.nhs.uk.

This information can be provided in other languages and formats if you are unable to read English. Please contact the Patient and Customer Services department and inform them of your preferred language. The department telephone number is 0161 419 5678. You could also email PCS@stockport.nhs.uk.

يمكن توفير هذه المعلومات في لغات وأشكال أخرى اذا كنت غير قادر على قراءة اللغة الانجليزية. الرجاء الاتصال بدائرة خدمات المريض والزبون وابلاغها بلغتك المفضلة. رقم هاتف هذه الدائرة هو 0161 419 5678. يمكن كذلك بعث بريدا الكترونيا الى PCS@stockport.nhs.uk-

আপনি যদি ইংরেজী পড়তে না পারেন তাহলে এই তথ্য অন্যান্য ভাষায় এবং ফরম্যাটে দেওয়া যেতে পারে। দয়া করে পেশেন্ট অ্যান্ড কাস্টমার সার্ভিসেস এর সাথে যোগাযোগ করে তাদের জানিয়ে দিন আপনার ভাষাটি। ডিপার্টমেন্টের টেলিফোন নম্বর 0161 419 5678, আপনি এছাড়াও ই-মেইল করতে পারেন PCS@stockport.nhs.uk এই ঠিকানায়।

如果您不能閱讀英語，這些資料是可以其他語言和格式來提供。請致電患者及客戶服務部門，並告知他們您的首選語言，該部門的電話號碼是 0161 419 5678，您還可以發送電子郵件至 PCS@stockport.nhs.uk –

اگر نمی توانید به زبان انگلیسی بخوانید، ما می توانیم این اطلاعات را به زبان ها و فرمت های دیگر در اختیار شما قرار دهیم. لطفا با دپارتمان Patient and Customer Services (خدمات مشتریان و بیماران) تماس بگیرید و زبان مورد نظر خود را به آنها بگویید. شماره تلفن دپارتمان 0161 419 5678 است. شما می توانید از طریق ایمیل نیز تماس بگیرید: PCS@stockport.nhs.uk

Te informacje mogą być udostępnione w innych językach i formatach jeśli nie potrafisz czytać po angielsku. Proszę skontaktować się z działem 'Patient and Customer Services' i poinformować ich o twoim preferowanym języku. Numer telefonu tego działu to 0161 419 5678. Możesz także wysłać email pod: PCS@stockport.nhs.uk

اگر آپ انگریزی نہیں پڑھ سکتے تو یہ معلومات دوسری زبانوں اور صورتوں میں بھی فراہم کی جا سکتی ہیں۔ براہ کرم پیشنٹ اور کسٹمر سروس والوں سے رابطہ کر کے اُنہیں بتائیں کہ آپ کونسی زبان میں معلومات چاہتے ہیں۔ اُن کا فون نمبر ہے 0161 419 5678۔ آپ اُنہیں PCS@stockport.nhs.uk پر ای میل بھی کر سکتے ہیں۔