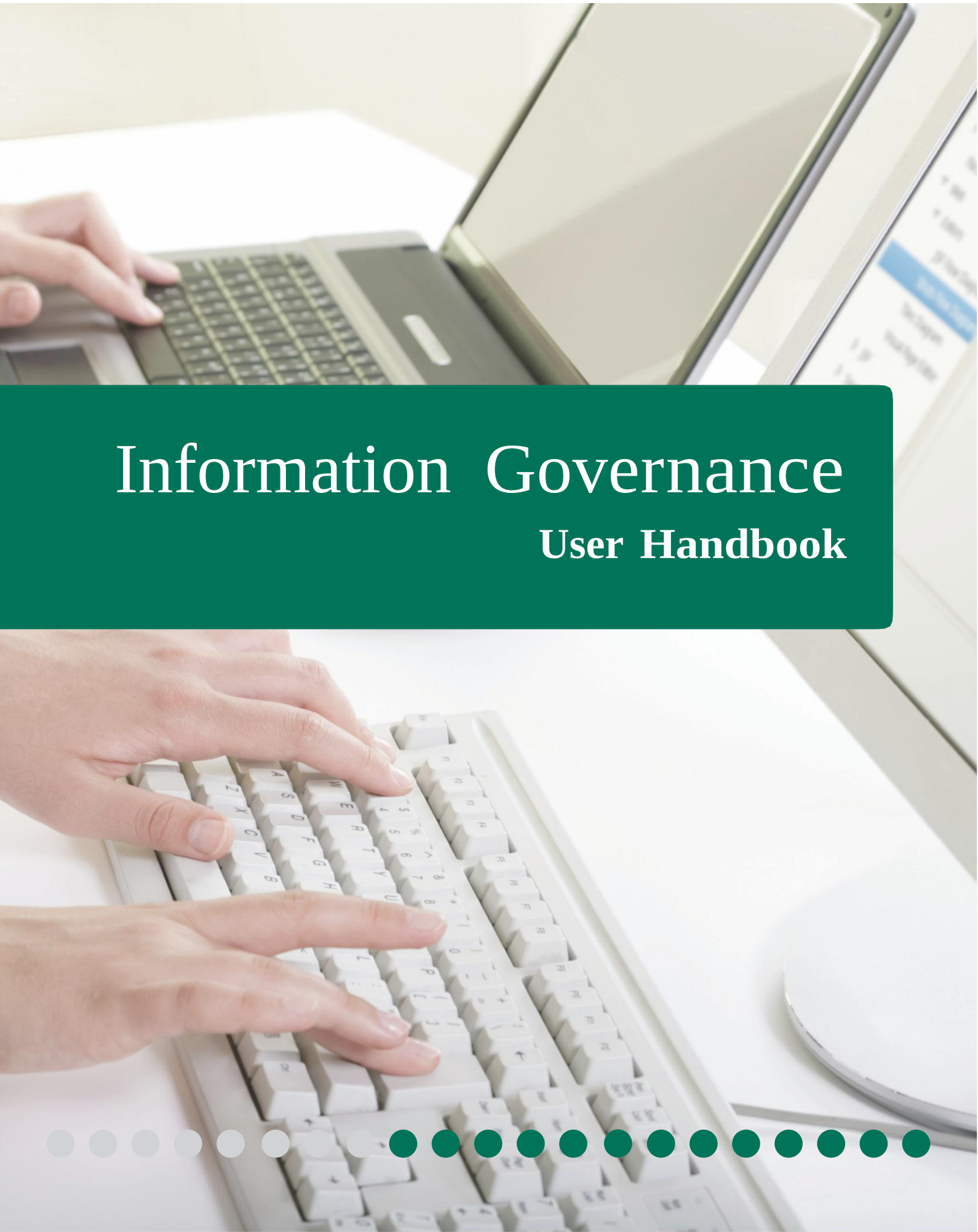

Information Governance

User Handbook

CONTENTS

1.0 INTRODUCTION TO INFORMATION GOVERNANCE

"Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information"

Health and Social Care – What you should know about Information Governance Booklet Pg 2
http://systems.hscic.gov.uk/infogov/links/igleaflet2010.pdf

Information Governance includes the following:

- Data Protection/Confidentiality
- Caldicott
- Information security
- Records Management and Data Quality.

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information plays a key part in clinical governance, service planning and performance management and therefore it is essential that all health organisations ensure information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Arrangements for secure disposal
- Used effectively and ethically, and
- Shared appropriately and lawfully.

1.1 How This Guidance Will Help You!

This guidance provides staff with a brief introduction to Information Governance and summarises the key user procedures that have been developed to support Information Governance in the organisation. The aim of this booklet is to ensure that you are aware of your roles and responsibilities for Information Governance.

Everyone in the organisation is responsible for Information Governance

2.0 KEY INFORMATION GOVERNANCE ROLES

A number of key Information Governance related roles are necessary within the organisational structure.

Senior Information Risk Owner (SIRO)

The SIRO is responsible for taking ownership of the organisations information risk policy and acts as an advocate for information risk at board or equivalent level.

Caldicott Guardian

The Caldicott Guardian takes an overarching responsibility for use of any patient identifiable information in the organisation.

Information Governance Lead

The Information Governance Lead is responsible for taking a lead role in Information Governance matters within the organisation.

Information Asset Owners (IAOs)

The Information Asset Owner is a senior manager who takes responsibility for the security of information of a specific information system or systems within the organisation, as well as understanding and taking ownership of the risks relating to the organisational assets and to provide assurance to the SIRO.

Information Asset Administrators (IAAs)

The Information Asset Administrator is responsible for the day to day running of one or more information systems and for ensuring that policies and procedures are adhered to, bringing any actual and/or potential risks to the attention of the IAOs.

3.0 INFORMATION GOVERNANCE POLICY

The purpose of the Information Governance policy is to set out the organisations IG Framework in order that appropriate processes and controls are put in place to protect the organisations information assets from all threats, whether internal or external, deliberate or accidental.

The Information Governance Policy of the organisation to ensure:

- Regulatory and Legislative requirements are met;
- Information is protected against unauthorised access;
- Appropriate policies and procedures are put in place to instruct staff in their responsibilities;
- Confidentiality of personal confidential information is assured;
- Integrity of the information and good data quality practices are maintained;
- Information is available to authorised personal when they need it in order to do their job;
- Information Governance Training is made available to and completed by all staff;
- Business Continuity and Disaster Recovery plans are produced, maintained and tested;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Governance Lead.

The policies and procedures produced to support the policy apply to this organisation and all its employees, executive and non-executive staff, agency staff, seconded staff and contractors.
The policies and procedures will be reviewed annually in accordance with the requirements of the Information Governance toolkit or upon significant internal/external changes and in conjunction with annual security audits. All staff will be informed of updates.

Policies which support the Information Governance policy will cover these areas:

- Access Control and Password Management
- Physical and Environmental Security
- Training
- Induction and Recruitment
- Network Security
- Registration Authority – this is the issue and management of smartcards
- Data Handling - Best Practice
- Exchanges of Information
- Email
- Internet
- Information Security Incident Management Procedures
- Business Continuity/Disaster Recovery Procedures
- Confidentiality and Data Protection
- Information Security and Safe Haven
- Information Sharing

It is the responsibility of each employee to adhere to the policy and underpinning procedures, to know where Information Governance policies can be accessed and to have read and understood them.

4.0 PERSONAL AND CONFIDENTIAL INFORMATION

What is personal information?

Personal confidential information is data from which a living individual could be identified; this could be about patients, careers, staff or any other individual about whom information is collected and processed, this may include information such as name, age, address, and personal circumstances. Some personal information is classed as **sensitive personal information** where it relates to an individual's: race, health condition, sexuality, etc.

The organisation places great emphasis on the need for the strictest confidentiality in respect of personal confidential data and especially on personal confidential information. This applies to manual and computer records and conversations about patients' treatments. **Everyone** working for the organisation is under a legal duty to keep personal information, held in whatever form, confidential. The patients and individuals who feel their confidentiality has been breached may raise a complaint under the organisations complaints procedure, etc.

The Duty of Confidence

All NHS Bodies and those carrying out functions on behalf of the NHS have a duty of confidence to those whose information they process, e.g. patients, staff etc.
Everyone working for or with the NHS who records, handles, stores or otherwise comes into contact with information that is capable of identifying any individual

The duty of confidence is upheld by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

The duty of confidence will also extend to other types of personal confidential information e.g. information provided by staff to the organisation for employment purposes. Additionally, some non-personal information may carry a duty of confidence such as those relating to contract tenders.

Protection of personal confidential data

Where personal confidential data is held then the organisation needs to take appropriate measures to ensure that it is secure and confidential. The organisation needs to take into account the sensitivity of the information as to what security measures are in place
Whenever possible, anonymised data should be used— from which all personal identifiers have been removed.

5.0 ACCESS TO PERSONAL INFORMATION

5.1 Staff access to personal confidential information

All staff should be aware that all access made to electronic records is recorded and auditable that audits are run periodically on all systems to check that access made to records is legitimate and required as part of a patient's healthcare pathway.

All staff are personally liable for breaches of the Data Protection Act 1998 and may be subject to the organisations disciplinary procedures and can be prosecuted in addition to the organisation itself being fined by the Information Commissioners Office

5.2 Individuals requesting access to personal confidential information

Individuals (such as patients or staff members) can request access to personal information held about them by the organisation, under the Data protection Act 1998, this is known as a Subject Access Request (SAR). The organisation will have a SAR process in place which all staff will need to be familiar with so that they know who to pass a request on to should they receive one.

6.0 SHARING AND USE OF PERSONAL INFORMATION

Information that can identify individual patients must not be used or disclosed for any other purpose than direct healthcare other than where:

- The individual patient or patients have given their explicit consent for the information to be used for specific purposes
- There is a legal obligation to disclose the information (e.g. Court Order)
- There is an overriding public interest to disclose the information e.g. to safeguard an individual, assisting a serious crime investigation.

Where any personal information is used or considered for use by the organisation, there must always be legal basis for that use. Where you share personal information with other organisation's, conditions must be adhered to as set out in the organisational Information Sharing Protocol.

7.0 INFORMATION GOVERNANCE USER PROCEDURES

7.1 Information Security – Staff Responsibilities

DO.....

- Remember that you have signed a confidentiality agreement within your contract of employment
- Be aware of information governance policies and procedures
- Be aware of your responsibilities for information security
- Be aware that unauthorised access to disclosure of or misuse of personal data will be treated as a serious disciplinary offence
- Ensure that temporary staff and third party contractors sign a confidentiality agreement available from the Information Governance Lead
- Ensure you receive appropriate training to enable you to carry out your work efficiently and securely
- Ensure your training needs are assessed on a regular basis
- Report potential weaknesses to your line manager
- Know how to report security incidents (see how to report an information security incident in section 7.12)
- Be aware that the organisation has a formal disciplinary process for dealing with staff that violate the organisations' policies and procedures.

DO NOT.....

- Attempt to prove a suspected security weakness, as testing a weakness might be Interpreted as a potential misuse of the system
- Allow third parties access to the organisations hardware and equipment, without correct authorisation
- Be afraid to challenge anyone who you were not aware would be in the organisation
- Ignore security incidents.

7.2 Physical security

DO.....

- Report the loss of your access keys or card immediately to your line manager
- Ensure all IT equipment is reasonably protected against theft and unauthorised access
- Follow the procedures for use of laptops, portable devices, mobile phones and removable media and ensure that if you use a blackberry, that it is password protected – see section 7.3 Use of Portable Devices
- Ensure that assets are disposed of in accordance with organisational policy
- Wear an ID badge
- Challenge unidentified visitors in controlled areas
- Escort visitors in secure areas at all times
- Operate a clear desk and clear screen policy
- Ensure confidential and patient information is locked away when not required
- Ensure that confidential waste is stored securely prior to disposal and certificates of destruction are obtained
- Ensure incoming and outgoing mail points are in secure areas
- Clear confidential and personal confidential information away from printers and fax machines immediately
- Ensure PC's are not left logged on and unattended—Ctrl-Alt-Delete, then click lock computer
- Ensure keys to premises are securely stored
- Ensure that secure areas are kept secure and locked when not in use
- Site computer screens away from unauthorised viewing
- Ensure that all deliveries are correctly checked, recorded and distributed in a secure manner.

DO NOT…..

- Take equipment, information or software off-site without prior authorisation
- Leave equipment unsecured in public areas
- Tell others what keys or access codes you have been entrusted with.

7.3 Environmental Security

DO.....

- Be aware of the building fire procedures
- Know who the fire officer is
- Attend a fire lecture on an annual basis or complete the mandatory e-learning module
- Keep fire doors closed
- Know where the fire extinguishers are
- Ensure that fire exits and manual fire alarms are accessible
- Maintain a neat and tidy environment to help limit the spread of fire Ensure that any heat source is always properly operated and maintained in accordance with fire regulations, this especially applies to electric cables Ensure that cabling does not trail and the electric source is not overloaded Label service and PC plugs to ensure that they are not accidentally unplugged Be vigilant for the risk of water damage.

DO NOT....

- Store flammables near to any source of heat
- Drink near the file server
- Site equipment near to sources of water e.g. radiators, water pipes, water tanks, air conditioning, pot plants, vase of flowers etc
- Attempt to tackle an outbreak of fire unless it is obvious that it can be easily extinguished by the appropriate hand held extinguisher.

7.4 User Access Control and password management

DO.....

Ensure that a user ID and password is required for access to the network and any applications containing personal information.

Select quality passwords with a minimum of eight characters which are:

- **Easy to remember**
- **notbased on anything somebody else could easily guess e.g. names, telephone numbers, date of birth etc**
- **a combination of upper and lower case letters, numbers and symbols**
- **not old or re-cycled passwords.**

Keep passwords confidential – **YOU are responsible for information entered using your password. Failure to protect YOUR password or workstation could result in disciplinary action.**

- Change passwords at regular intervals (and also if there is any indication of a possible systemor password compromise)
- Use password protected screensavers when away from your desk **(activated by ctrl+alt+del, then click lock computer)**
- Be aware that you are responsible for any activity performed under your logon ID and password. This includes any activity undertaken by someone else whilst your PC is left logged in and unattended without a password protected screensaver
- Ensure that you log off correctly (i.e. don't just switch the machine off)
- Contact if you have forgotten your password and need your access to be reset
  If you are a line manager - terminate a staff member's network access or smartcard rights
- when they leave your organisation.

DO NOT…..

- **Leave a PC logged in and unattended (activate Ctrl-Alt-Del, then click lock computer) to secure your PC**
- **Use someone else's ID or login or allow anyone to use yours (this is a serious disciplinary offence and all access is auditable)**
- **Write a password down (unless you can store it securely)**
- **Connect any unauthorised hardware or download software to the organisation network.**

7.5 Use of portable IT devices

Portable devices include laptops, notebooks, tablet computers, PDA's (personal digital assistants), cameras and mobile phones.

Removable data storage media include any physical item that can be used to store and/or move information. This could be a USB stick, CD, DVD, floppy disc, tape, video or camera memory cards or digital storage devices.

Unencrypted personal data held on portable devices present a **huge risk** to the organisation if lost or stolen.

YOU MUST ENSURE THAT:

- Only authorized staff have access to portable computer devices and digital storage devices such as USB's etc. All portable equipment that contains personal and confidential information **must** be encrypted. There are no exemptions to this rule and you will be held personally responsible if you download such data to an unencrypted device. If you are unsure whether your device is encrypted please contact the service helpdesk.
- A register is maintained where portable equipment is used in a pool to enable the identification of the current user
- Any backups taken from portable devices should always be encrypted to NHS standards and stored securely
- Any loss or theft of portable equipment is reported immediately to the police and your line manager
- If you have been issued with an encrypted laptop for use in your organisation, you must log the laptop onto the network at least once every three months to ensure that the encryption password remains valid.
- Use portable media for short term storage only - ensure it is backed up to the server frequently.

DO NOT....

- Store identifiable information on removable media unless it is absolutely necessary and
- if so, ensure it is password protected and encrypted
- Leave portable equipment in places vulnerable to theft
- Leave equipment unattended in public areas
- Leave portable equipment visible in a car, always lock it away in the boot
- Delay in reporting any lost or stolen equipment to the police and your manager Connect any unauthorised equipment to the network mp3 players, cameras, wireless routers—if in doubt, contact the IT service desk
- Install unauthorised software or download software from the internet without authorisation from IT.
- Allow unauthorised personnel to use the equipment, e.g. household members

7.6 Terms and conditions of use of smartcards

Individual smartcards are issued to organisation team members who require access to specific clinical systems. Smartcards provide you with the appropriate level of access to healthcare information that you need to do your job.

Remember – You have a duty to keep patient information secure and confidential at all times and the terms and conditions of use mean that you:

DO.....

- Read and follow the declarations set out in the RA01 short form conditions for smartcard users
- Understand that NHS smartcards help control who accesses what and at what level. Using the same technology as chip and pin, members of staff are identified by names, by photograph and a unique identity number.

DO NOT

- Share individual smartcards
- Allow anyone to use your smartcard—checks on access will be made and you will be held responsible for all patient data accessed and or recorded using your smartcard
- Leave your smartcard unattended at any time
- Access any record / information you do not have a legitimate right to access.

7.7 Protection against malicious software

DO.....

- Ensure your PC will have anti-virus software, this needs to be operating and up to date.

On discovering a virus:

- Note any symptoms and immediately shut down the PC
- **Contact the IT service desk immediately**
- Ensure that electrical appliances are checked annually.

DO NOT....

- Attempt to clear an infected PC yourself
- Accept any freeware as it may contain spyware or a virus
- Review to ensure all relevant items detailed e.g emails

7.8 Software, data and media management

DO.....

- Respect all computer software copyrights and adhere to the terms and conditions of any licence to which the organisation is a party
- Actively and frequently undertake housekeeping of your data, e.g. delete unwanted files regularly as information is soon out of date
- Archive files and documents on a regular basis in line with your retention policy or in line with the NHS Records Management, Code of Practice
- Clear all patient or confidential information off disks and tapes reformatting (not by deletion) before disposing
- Ensure that tapes and disks are disposed of securely, contact IT Services for support

7.9 Data handling

DO.....

- Lock any manual patient records, such as Lloyd George envelopes away when not in use
- Ensure that confidential conversations are held where they cannot be overheard by members of the public or other staff and ensure that sensitive medical issues are only discussed in private consultation areas
- Encrypt any confidential/sensitive information which needs to be emailed from the organisation unless sending nhs.net to nhs.net. In the case of sending of extremely sensitive information consider sending a test email first
- Ensure that all waste containing patient or staff identifiable information is cross shredded before disposal using shredding consoles
- Be aware of safe haven guidelines for confidential information e.g.faxes but if possible try to use nhsmail instead.

- **Contact the recipient to let them know that the fax is being sent**
- **Check the number dialled and check again before sending**
- **Where possible use pre-stored numbers**
- **Ask the recipient to acknowledge receipt**

- Take care when making a phone call to ensure that you do not reveal **confidential Information e**g by being overheard
- Take care when listening to answer phone messages e.g. close the door when retrieving messages
- Ensure that envelopes containing personal confidential data sent via internal or external mail are clearly and correctly addressed, marked 'confidential' and the senders address included

DO NOT…..

- Leave information where it can be viewed by someone who does not have a legitimate right to view it
- Discuss patient or staff details where you may be overheard
- Disclose information to someone where there is not a legal basis to do so.
- Leave confidential messages on answering machines or text patients without their explicit consent.

7.10 Email use

DO.....

- Be aware that the email system is primarily for business use. Occasional and reasonable personal use is permitted provided that it does not interfere with the performance of your duties and does not conflict with organisational policies
- Be aware that the organisation may inspect email addresses and contents (including personal email) without notice. Follow the email procedures for email etiquette, acceptable use and the retention of messages
- Be aware that the same laws apply to email as to any other written document
- Use an auto signature which must include your contact details e.g. name, telephone number and work address
- Be careful about content - email is easily forwarded
- Use out of office assistant to advise people when you are not available
- Ensure email delegates are set up appropriately, to allow access to your emails whilst out of the office, on holiday etc
- Use the address book (or contacts) where possible, to prevent incorrect addressing
- Report to your Line Manager or Information Governance Lead any email that you receive, or become aware of, that may be regarded as illegal or offensive
- Be aware that your mailbox may be opened to access information if absent, e.g. sickness or holiday
- Remove any personal contents from your mailbox and personal network folders when leaving employment; (it may be made available to a replacement or line manager)
- Personal, sensitive or confidential information must be sent by secure email e.g. NHS.net to NHS.net

DO NOT…..

- Send sensitive or confidential information via an insecure email address unless it is encrypted
- Attach large files to emails (+10mb) - where possible send a link to the file or WinZip it to reduce its size
- Send email that is or which could be considered to be sexually or racially offensive, pornographic, defamatory, abusive, criminal or for any other unauthorised purpose Create or forward chain email
- Send emails to large numbers of people unless it is directly relevant to their job.
- Set up an auto-forward of your work emails to a home email address i.e. hotmail, yahoo
- Do not use your email account for permanent storage of work related issues.

7.11 Internet use

DO.....

- Be aware that the use of the internet is primarily for business use unless otherwise agreed with your employer and that all use may be monitored
- Be aware that any inappropriate use of the internet may result in prosecution and/ or disciplinary action being taken against you
- Be aware of the social media procedures e.g. obtain approval from your line manager for any online activities associated with the work of the organisation, e.g. by displaying an your organisations email address or Trust related network on social networking sites (such as facebook) or by making reference to the organisation as your employer.

DO NOT…..

Leave the internet logged in and unattended
View, download, transmit or save any information, graphics, photos, software, music, video clips unless it is relevant to your role and you have been given permission to do so by the organisation.

7.12 Information Security Incident Management

Information security incidents are any event that has resulted or could have resulted in the disclosure of confidential information to an unauthorised individual, the integrity of the system or data put at risk or the availability of the system or information being put at risk. Incidents may include theft, misuse or loss of equipment containing confidential information or other incidents that could lead to unauthorised access to data all of which will have an adverse impact to patients and to the organisation e.g.

- embarrassment to the patient/patients/organisation
- threat to personal safety or privacy
- legal obligation or penalty
- loss of confidence in the organisation
- financial loss
- disruption of activities.

All incidents, or information indicating a suspected incident should be reported as soon as possible to your organisation's Information Governance Lead. Details of incidents must be reported via the organisations' risk incident reporting procedure. Breach of data security must be reported to the Governing Body and the SIRO.

DO NOT…..

- Keep an incident to yourself, ensure it is reported so that working practices can be improved.

7.13 Serious Incidents Requiring Investigation (SIRI)

Incidents that are classed as Serious Incidents require additional reporting processes.
An Information Governance SIRI would be where for example there is significant loss of personal information involving a large number of people or where particularly sensitive personal information has been sent to the wrong person or location. Where staff become aware of a SIRI they should inform the organisations Information Governance Lead who will report the incident to the Strategic Executive Information System (STEIS). Breaches of data security must also be eported at Board level and to the SIRO.

An Information Governance related SIRI also needs to be reported on the organisations Information Governance online Toolkit. The Information Governance Toolkit administrator and/or nominated staff will report this by accessing the Incident Reporting tool within the Information Governance Toolkit.

8.0 COMPLIANCE REQUIREMENTS

DO.....

- Be aware that the organisation is obliged to abide by relevant UK and EU Legislation - the key ones are listed below:

Key legislation and guidance

- Data Protection Act 1998
- Access to Health Records Act 1990
- The Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1998
- Human Rights Act 1998
- The Caldicott P rinciples.
- The Health and Social Care Act 2012 (Includes sections on access to confidential information)
- The NHS Care Record Guarantee

DO NOT…..

- Breach legal requirements
- Be ignorant of the legal requirements that affect you
- Copy software or documents illegally or breach copyright laws.

8.1 Data Protection Act 1998

The Data Protection Act 1998 (DPA) aims to promote high standards in the handling of personal confidential information. The Information Commissioner is responsible for enforcing the DPA which applies to anyone holding personal confidential information about living individuals.

The DPA requires organisations:

To notify the Information Commissioner you are processing personal information.

To process the information in accordance with the eight principles of the DPA, information must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of the data subject
- Kept secure
- Not transferred to other countries without adequate protection.

The organisation needs to collect personal information about people with whom it deals with in order to carry out its business and provide services. Such people include patients, employees, suppliers and other business contacts. The information includes name, address, email address, date of birth, private and confidential information, sensitive information and business sensitive information.

In addition, the organisation may also collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the DPA. If an organisation holds information on you, you are classed as a data subject. All data subjects have a right to confidentiality under the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality.

Data subjects can also request a copy of all the information you hold on them but any request must be made in writing (also see section 5 - Access to personal information).

The organisation must provide the information within 40 days ensuring that checks are made as to the identity of the requester and removing any third party information or information which may cause harm or distress to the requester or anyone who may see it.

New powers designed to deter data breaches came into force on the 6th April 2010. The Information Commissioner's Office (ICO) is able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. The power to impose a monetary penalty is designed to deal with the most serious personal data breaches and is part of the ICO's overall regulatory toolkit which includes the power to serve an enforcement notice and the power to prosecute those involved in the unlawful trade in confidential personal data. ***www.ico.gov.uk***

8.2 The Caldicott Principles

The December 1997 Caldicott Report identified weaknesses in the way parts of the NHS handle confidential patient data. The report defined six Caldicott principles which provide a framework for the management of access to personal information within the NHS.

A review of Caldicott has been undertaken, known as Caldicott 2 where a revised set of principles have been recommended, see below:

Follow the Caldicott principles:

Principle 1: **Justify the purpose(s) (for using confidential information)**

Principle 2: **Don't use personal confidential data unless it is absolutely necessary**

Principle 3: **Use the minimum necessary personal confidential data**

Principle 4: **Access to personal confidential data should be on a strict need-to-know basis**

Principle 5: **Everyone with access to personal confidential data should be aware of their responsibilities**

Principle 6: **Comply with the law**

Principle 7: **The duty to share information can be as important as the duty to protect patient confidentiality**

8.3 HSCIC Confidentiality rules

In September 2013 the Health and Social Care Information Centre (HSCIC) defined five confidentiality rules in their guide 'A guide to confidentiality in health and social care' which set out to demystify the complexities between the law, professional obligation and a duty of care towards the individual, see below:

Rule 1: **Confidential information about service users or patients should be treated Confidentially and respectfully**

Rule 2: **Members of a care team should share confidential information when it is needed for the safe and effective care of an individual**

Rule 3: **Information that is shared for the benefit of the community should be anonymised**

Rule 4: **An individual's right to object to the sharing of confidential information about them should be respected**

Rule 5: **Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed**

8.4 Business Continuity

Ensuring that the organisation has a robust plan to mitigate disruptions to its business are paramount in providing a reliable service to its customers.

Business continuity planning enables the organisation to:

- Assess the risk of a security failure or disaster occurring
- Analyse the consequences to the running of the organisation if a security failure or disaster was to occur
- Plan measures to reduce the likelihood of a security failure or disaster occurring
- Identify critical resources
- Plane measure to allow the organisation to continue to function if a security failure or disaster does occur.

DO.....

- Identify your critical business resources
- Take preventative measures to guard against the likelihood of an incident occurring or having a major incident
- Decide what takes priority for recovery
- Have emergency contacts handy and up to date
- Prepare contingency plans for the most likely emergency situations
- Practice your plans on a regular basis
- Make sure everyone knows what to do and when
- Keep plans up to date by informing a change of contact details etc
- Seek help and guidance for preparing and evaluating your plans
- Record any incidents which resulted in you testing the plan i.e. loss of electricity/gas supply.

DO NOT…..

- Think it will never happen to me
- Think that it is someone else's problem
- Make plans that are too difficult to follow
- Create a plan, and forget about it. It must be kept up to date to be useful
- Keep plans where you can't get to them, ensure you have one copy on site and one copy off site
- Use unrealistic scenarios for testing the plan e.g. a meteor landing on the building.

9.0 TOP TIPS FOR PROVIDING A CONFIDENTIAL SERVICE

Remember, information governance is common sense. Don't take risks with information always handle it as if it were your own.

Don't put yourself or your organisation at risk. The harm you may cause to patients/clients may result in a claim against you or your employer. The Information Commissioner can also fine organisations up to £500k if information is recklessly lost or disclosed without due regard to policies and procedures.

Think about all information as if it were your own would you expect your information to be left available for anyone to view?

- **Lock your workstation:** When leaving your work station always LOCK YOUR PC—get into the habit of pressing **Control-Alt-Delete-Return** (lock computer), whenever you leave your desk. Remember, any work done under your login will be attributable to you— even if you did not do it!
- **Passwords: NEVER** share your login or password or use anyone else's login or password
- **Smartcards: NEVER** leave your smartcard unattended—**ALWAYS REMOVE IT** when leaving your workstation. As above—remember any work done under your login will be attributable to you—even if you did not do it!
- **Faxes:** When faxing personal or patient identifiable information always use a safe haven fax machine or safe haven fax procedures. Full safe haven procedures are available in the organisation
- **Emails: ALWAYS ENCRYPT PERSONAL IDENTIFIABLE OR BUSINESS SENSITIVE DATA** When sending via email
- **Paper information:** Think about how you handle paper information as if it were your own information e.g. diaries, patient lists, letters, would you leave your information on view for anyone to see— **ALWAYS** secure any information you are handling
- **Memory sticks (USB's):** It is policy that only supplied encrypted memory sticks (safesticks) are used for business purposes. Any existing unencrypted sticks must no longer be used to save information to and passed to IT for safe destruction
- **Post:** Patient identifiable information sent from the organisation via Royal Mail should always be marked 'Private and Confidential'and sent securely.

If sending more than 20 items in one envelope, ensure that the envelope is robust and use either an approved courier service or a secure postal service, such as recorded.

10.0 INFORMATION GOVERNANCE TRAINING

Remember, it is your responsibility to ensure that your Information Governance Training is kept up to date