NHS
Dudley
Clinical Commissioning Group

Information Reader Box	
Dudley CCG	
Purpose	Guidance
Document Purpose	Procedures
Document Name	Information Governance Handbook
Author	Information Governance Team CSU
Publication Date	07/01/15
Review Date	26/09/15
Target Audience	All working for or on behalf of Dudley CCG
Description	Procedures for Information Governance
Cross Reference	Information Governance Policy
Superseded Document	N/A
Action Required	To Note
Approved by	CCG Audit Committee 26/09/15
Contact Details (for further information)	Midlands and Lancashire CSU Information Governance Team informationgovernance@staffordshirecss.nhs.uk / information.governance@lancashirecsu.nhs.uk 01254 282999

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet http://intranet.dudleyccg.nhs.uk/policies/app/Home.aspx is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet http://intranet.dudleyccg.nhs.uk/policies/app/Home.aspx

Version	Date	Author	Changes
V1	26/09/14	CSU IG	Version & Date details

CONTENTS

INTRODUCTION

This handbook is designed to provide a central place for all staff to access the Information Governance Procedures they are required to work to in order to ensure compliance with Information Governance legislation and national and local guidance.

SCOPE

This handbook covers all aspects of information within the organisation, including but not limited to personal information and organisational information. The handbook should be used by all staff when using, handling, processing and storing information. This includes temporary staff, contractors and students working for the organisation.

MONITORING

The organisation will monitor the handbook through the Audit Committee. Staff compliance with the handbook will be monitored through regular staff compliance checks, incident reports and the information risk assurance work programme. Failure to comply with the handbook will be dealt with as a serious breach of policy and could lead to disciplinary action being taken.

Staff should also be aware of their own personal liability as a result of the Information Commissioners Office powers. Should a member of staff cause a data breach through failure to follow the organisations policies and the IG handbook, they could face a fine of up to £500,000.

All staff have a responsibility to ensure that if they are unable to comply with any part of the handbook that they notify the Information Governance Team immediately to allow for an alternative solution to be approved. Information Governance is everyone's responsibility!

WHAT IS INFORMATION GOVERNANCE?

Good professional practice goes hand in hand with 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, allowing:

- ✓ Implementation of central advice and guidance;
- ✓ Compliance with the law;
- ✓ Year on year improvement plans.

At its heart, Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

Information is a vital asset to the organisation but it also poses one of our greatest risks. It is therefore essential that as an organisation, when information is used, that it is handled in accordance with this handbook. This will ensure that all relevant legislative requirements are met.

POLICY AWARENESS AND COMPLIANCE

The CCG has a responsibility to ensure that all staff are aware of the expectations placed upon them regarding how they use the information they come in to contact with as part of their work for the CCG.

This may be information which identifies individuals, or which is "commercially sensitive" and would be detrimental to the organisation if its confidentiality was breached.

Therefore, the CCG has put in place an IG policy alongside this handbook which cover all aspects of Information Governance and will provide guidance and direction on how staff are expected to work with confidential information, and in doing so, ensure compliance with all relevant legislation.

These documents are available to all staff at:
http://intranet.dudleyccg.nhs.uk/policies/app/Home.aspx

It is particularly important that every effort is made to follow this guidance as the Information Commissioner's Office (the body who regulate compliance with the Data Protection Act and Freedom of Information Act in England) has the power to fine both organisations and **individuals** up to **£500,000** if a serious enough breach of the Data Protection Act occurs.

In addition to this, at an organisational level, any breaches of the IG policy or handbook may result in disciplinary procedures.

THE LEGAL FRAMEWORK

The CSU has a responsibility to ensure that all staff are aware of the legislation and best practice that governs the use of personal information.

THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 regulates the processing of information about living individuals including the obtaining, use and disclosure of information and sets out the rights and responsibilities of data subjects and data users. It covers all paper and computer records.

The Data Protection Act states that anyone who processes personal data must comply with the 8 principles contained in Section 1 of the Act. Processing means anything that is done with personal information – including, but not limited to, collecting, storing, sharing and destroying it. The following summary sets out the implications for all staff.

Principle 1: Personal data shall be processed fairly and lawfully

The aim of this principle is to ensure that personal data is processed fairly and lawfully and in accordance with a relevant condition from the schedules of the Act. Information given in confidence must not be disclosed without the consent of the giver of that information.

Compliance will be achieved by implementing the following measures:

- All staff will have a confidentiality clause in their contract of employment. A "contract, temporary and work placement staff confidentiality and compliance agreement" is included in Appendix J of this handbook.

- All users of records, IM&T equipment and systems are required to sign a written agreement.

- Third party contractors working for the organisation are required to sign a confidentiality agreement before they are connected to the IT networks.

- Informing staff, patients/service users how their data will be processed. This means fully describing how the data will be used and for what purposes.

Principle 2: Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

If personal data has been lawfully collected for a specific purpose, that data cannot then be used for an additional or new purpose without establishing a legal basis to do so, e.g. gain further consent from the data subjects concerned.

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

It must be ensured that whenever gathering personal data, it is relevant, adequate and not excessive for the intended purpose.

The organisation will ensure that systems and processes ensure only relevant information is captured and processed. The organisation will implement 'need to know' access controls and will conduct routine audits as part of good data management practice.

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

All staff who record personal data are responsible for its quality. The data must be **C**omplete, **A**ccurate, **R**elevant, **A**ccessible and **T**imely.

This also applies to staff data so it is the responsibility of each member of staff to notify the CSU of any changes in their personal circumstances, for example, change of address.

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Records containing personal data must be retained and disposed of in line with NHS guidance. For further detail of this please refer to the “Records Management” section of this handbook.

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under this Act.

Under the Data Protection Act, individuals have the following rights:

- Right of subject access
- Right to prevent processing likely to cause harm or distress
- Right to prevent processing for the purposes of direct marketing
- Right in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

Principle 7: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

The organisation will ensure that both physical and technical security measures and procedures are in place to protect current and archived records. These measures are subject to continual review and risk assessment through the Information Risk Assessment and Management Programme detailed in this handbook.

The organisation will ensure that the sharing of personal identifiable information, data and software exchange conforms to protocols, including disclosure in line with statutory requirements.

Principle 8: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

As countries outside of the EEA may not have comparable Data Protection legislation and controls to the UK, should there be a need to transfer personal data to another country, please contact your Information Governance Support Officer for guidance.

Further information regarding all of the Data Protection Act principles can be found on the ICO website www.ico.gov.uk

Exemptions to the Data Protection Act 1998

Personal information must not be disclosed to third parties without the data subject's informed consent, except in very limited circumstances. This could include:

1. Statutory obligation, e.g. a court order
2. Legislation, e.g. Children's Act 2004, Mental Capacity Act 2005
3. The receiver holds a section 251 approval which allows them to collect PCD without requiring any further consent

If in doubt, staff must seek guidance from the CSUs Information Governance team and the Caldicott Guardian. In complex cases the organisation will seek expert guidance from legal advisers.

CALDICOTT PRINCIPLES

All staff must be aware of, and comply with the following Caldicott Principles for handling person confidential data (PCD):

- **Principle 1: Justify the purpose(s)**

Every proposed use or transfer of PCD within or external to the organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the Caldicott Guardian.

- **Principle 2: Don't use patient identifiable information unless absolutely necessary**

PCD should only be used if there is no alternative.

- **Principle 3: Use the minimum necessary patient identifiable information**

Where use of PCD is considered to be essential - use only that information necessary to achieve the purpose.

- **Principle 4: Access to patient identifiable information should be on a need to know basis**

Only those individuals who need to access PCD should have access to it, and they should only have access to the information items they need to see.

- **Principle 5: Everyone should be aware of their responsibilities**

Action should be taken to ensure that those handling PCD are aware of their responsibilities and obligations to respect patient confidentiality.

- **Principle 6: Understand and comply with the law**

Every use of PCD must be lawful

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

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

NHS CODES OF PRACTICE

There are many “Codes of Practice” which explain how information should be used in the NHS, including:

- **The ‘Confidentiality: NHS Code of Practice’**

The 'Confidentiality: NHS Code of Practice' sets out the required standards of practice concerning confidentiality and patients' consent to use their health records.

It is a guide for those who work within or under contract to NHS organisations and is based on legal requirements and best practice.

- **The ‘Information Security Management: NHS Code of Practice’**

The 'Information Security Management: NHS Code of Practice' is a guide to the methods and required standards of practice in the management of information security, for those who work within or under contract to, or in business partnership with NHS organisations in England.

- **The ‘Records Management: NHS Code of Practice’**

The ‘Records Management: NHS Code of Practice’ sets out standards required for the management of NHS records and applies to hard copy and digital records

NHS CARE RECORD GUARANTEE FOR ENGLAND

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this.

It covers people's access to their own records; controls on others' access; how access will be monitored and policed; options people have to further limit access; access in an emergency; and what happens when someone cannot make decisions for themselves.

Everyone who works for the NHS, or for organisations delivering services under contract to the NHS, has to comply with this guarantee.

A Guide to Confidentiality in Health and Social CARE

Organisations that handle confidential health and social care information have to ensure that it is held securely and shared appropriately.

A number of laws, principles and obligations govern how organisations should handle this information. They have grown increasingly complicated to understand and this has sometimes made it hard for staff to make clear decisions about when they should and should not share confidential information.

The Health and Social Care Information Centre have produced a guide to confidentiality in health and social care which explains the various rules about the use and sharing of confidential information. It has been designed to be easily accessible and to aid good decision making. It also explains the responsibility organisations have to keep confidential information secure.

The guide is supported by a references document which provides more detailed information for organisations and examples of good practice.

NHS CONSTITUTION

The constitution sets out rights for patients, public and staff. It outlines NHS commitments to patients and staff, and the responsibilities that the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively. All NHS bodies and private and third sector providers supplying NHS services are required by law to take account of this constitution in their decisions and actions.

KEY ROLES IN INFORMATION GOVERNANCE

SENIOR INFORMATION RISK OWNER – CHIEF FINANCE OFFICER

The Senior Information Risk Owner (SIRO) is an Executive Director of the Board. The SIRO is expected to understand how the strategic business goals of the Governing Body may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions, and will provide written advice to the Accountable Officer on the content of their Annual Governance statement in regard to information risk.

The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Governing Body and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the Information Governance team and the Caldicott Guardian, although ownership of the Information Risk programme will remain with the SIRO.

The SIRO will be supported through a network of Information Asset Owners and Administrators who have been identified and trained throughout the organisation

CALDICOTT GUARDIAN – CCG BOARD MEMBER

The Caldicott Guardian has particular responsibility for reflecting patients' interests regarding the use of patient identifiable information and to ensure that the arrangements for the use and sharing of clinical information comply with the Caldicott principles. The Caldicott Guardian, supported by Caldicott Leads and Assistants, will advise on lawful and ethical processing of information and enable information sharing. They will ensure that confidentiality requirements and issues are represented at Governing Body level and within the overall governance framework.

INFORMATION ASSET OWNERS AND INFORMATION ASSET ADMINISTRATORS

As part of the SIRO framework, individuals across the organisation will be nominated to perform the roles of either Information Asset Owner (IAO) or Information Asset Administrator (IAA). These individuals will be identified initially by their department leads with further nominations being made by IAOs as required.

The IAO role must be an accepted part of any departmental management structure in much the same way as a budget holder. IAOs are senior individuals involved in running the relevant team. Their role is to understand and address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of these assets.

The IAA role is to provide support to each IAO and to ensure that information asset registers are populated accurately and maintained regularly.

INFORMATION GOVERNANCE TRAINING

To ensure organisational compliance with the law and central guidelines relating to Information Governance, staff must receive appropriate training. Therefore, IG training is mandatory for all staff and staff IG training needs should be routinely assessed, monitored and adequately provided for.

Information Governance knowledge and awareness should be at the **core** of the organisations objectives, embedded amongst other governance initiatives and should offer a stable foundation for the workforce. Without this knowledge, the ability of an organisation to meet legal and policy requirements will be severely impaired.

Therefore, to meet these requirements the organisation has established a clear plan for IG training which is outlined below.

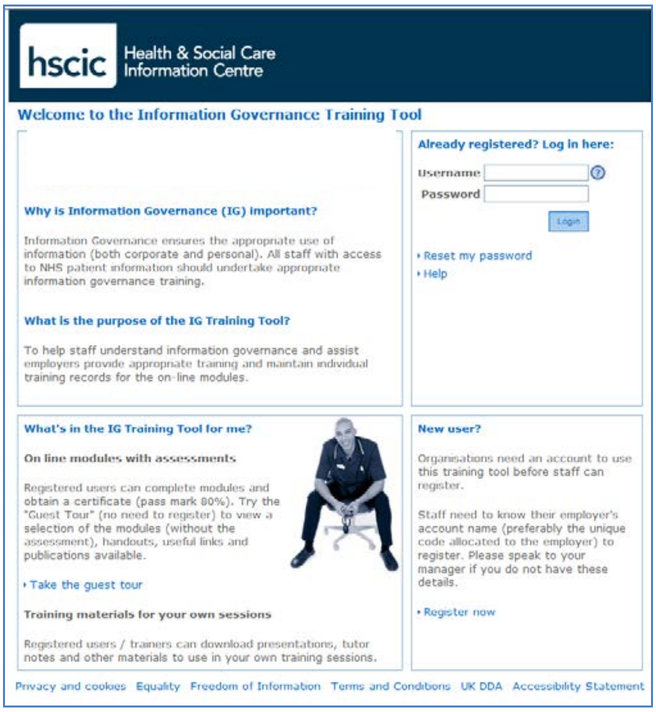
INFORMATION GOVERNANCE INDUCTION

It is vitally important that **all new staff** are made aware of the organisations Information Governance requirements at the earliest opportunity and clear guidance is given about **their own individual responsibilities for compliance.** Particular emphasis must be placed on how IG requirements affect their day to day work practices. It is equally imperative that IG remains embedded with each individual throughout their daily working practices.

Line Managers should ensure that new starters receive an initial IG induction using the checklist which can be found at Appendix A of this handbook on their first day of employment, with a further 1-1 induction with the CCGs Information Governance Support Officer using the checklist at Appendix B within the first 2 weeks.

Further to the face to face inductions, it is mandatory for all NHS staff (including locums, temporary, student and contract staff) to undertake the “Introduction to Information Governance” module of the online e learning tool within one month of commencing employment.

The IG Training Tool can be accessed at **https://www.igtt.hscic.gov.uk/igte/index.cfm**



Welcome to the Information Governance Training Tool

Why is Information Governance (IG) important?

Information Governance ensures the appropriate use of information (both corporate and personal). All staff with access to NHS patient information should undertake appropriate information governance training.

What is the purpose of the IG Training Tool?

To help staff understand information governance and assist employers provide appropriate training and maintain individual training records for the on-line modules.

Already registered? Log in here:

What's in the IG Training Tool for me?

On line modules with assessments

Registered users can complete modules and obtain a certificate (pass mark 80%). Try the "Guest Tour" (no need to register) to view a selection of the modules (without the assessment), handouts, useful links and publications available.

Training materials for your own sessions

Registered users / trainers can download presentations, tutor notes and other materials to use in your own training sessions.

New user?

Organisations need an account to use this training tool before staff can register.

Staff need to know their employer's account name (preferably the unique code allocated to the employer) to register. Please speak to your manager if you do not have these details.

On registering for an account on the IGTT you will be asked for the organisation code.

Organisation Codes are:

Dudley CCG	05C

Following **successful** completion of the Induction module on the IG training tool, all new starters will then need to book on the first available IG refresher training session (please see “Mandatory Information Governance Training” section of this handbook).

MANDATORY INFORMATION GOVERNANCE TRAINING

Following the initial training completed during the first month of employment, subsequent refresher training will be delivered through face to face training sessions. These sessions will be provided throughout the year and it is the responsibility of every individual to attend one the training sessions. These sessions are interactive sessions which, alongside ensuring that staff are fully informed of CCG specific working practices, will test staff understanding and compliance. This will allow any further training needs to be identified.

Failure to attend the face to face sessions will result in the individual having to complete online e-learning modules in order to maintain their individual compliance. In addition, anyone who is unable to attend a face to face session will be required to evidence their compliance with CCG specific working practices, policies and procedures through additional spot checks.

SPECIALIST INFORMATION GOVERNANCE TRAINING

Through the results of spot checks, appraisals and other reviews of staff understanding and compliance with IG procedures, it may be identified that some staff groups or individuals require further training in order to fulfil their role.

INFORMATION RISK

Adequate information security management and assurance arrangements are needed to ensure the organisation complies with its information security obligations and keeps the Board informed of changes and performance issues which need to be considered and addressed. To achieve this, the organisation has implemented a Senior Information Risk Owner (SIRO) framework.

The individual nominated to act as Senior Information Risk Owner for the organisation will be required to successfully complete strategic information risk management training at least annually. This should be achieved by their completion of the “NHS Information Risk for SIROs and IAOs” module of the NHS IGTT. Further updates will be provided by Information Governance.

The nominated IAOs and IAAs will be required to attend Information Risk training provided by the Information Governance team. This training will ensure that attendees have a full understanding of:

- ✓ The background to the SIRO framework
- ✓ The importance of information risk management and the potential consequences if things go wrong
- ✓ What the roles of IAO and IAA mean and the expectations and responsibilities that are placed on individuals performing these roles
- ✓ How to complete Information Asset registers and Data Flow mapping exercises.

Information Risk Training should be undertaken on an annual basis. This is due to the number of changes that occur within a 12 month period in relation to Information Risk.

PRIVACY IMPACT ASSESSMENT TRAINING

The organisation must ensure that when new projects, processes, services or systems are introduced, or changes made to existing ones, the implementation does not breach information security, confidentiality or data protection requirements.

To assist with this, the Information Commissioners Office (ICO) has developed a framework called a Privacy Impact Assessment (PIA) for use when developing and introducing projects and processes that may have an impact on how we use patient and staff information. This process enables organisations to anticipate and address the likely impacts of new initiatives on an individual's privacy.

Any staff who may be involved in the management of new projects or processes for the organisation will be offered training on the Privacy Impact Assessment process. This training will be provided by the Information Governance team. This is a group training session which will cover:

- ✓ Why the PIA process was introduced
- ✓ Identifying when a PIA should be considered
- ✓ The stages of a PIA
- ✓ What should be included when conducting a PIA
- ✓ How to document the PIA process

CALDICOTT & DATA PROTECTION TRAINING

Confidentiality and Data Protection is a key element of the Information Governance agenda. The recommendations of the Caldicott Committee (1997 Caldicott Report and 2013 Information Governance Review) defined the confidentiality agenda for Health and Social Care organisations. A key recommendation was the appointment in each NHS Health and Social Care organisation of a "Guardian" of patient identifiable information to oversee the arrangements for the use and sharing of patient information. Caldicott Guardians were mandated for the NHS in Health Service Circular 1999/012.

To enable them to fulfil their role of Caldicott Guardian, the nominated individual will be required to complete accredited training on a three yearly basis. This should be achieved by their completion of the "The Caldicott Guardian in the NHS and social care" module of the NHS IGTT or by an agreed external training organisation.

The organisation has assessed its confidentiality and data protection obligations and associated risks to determine the resources needed to establish and maintain the level of assurance required. It has been identified that as some areas of the organisation process person confidential information, a Subject Access Lead will be appointed and trained to support the Caldicott Guardian in their function.

The Subject Access Lead will be required to complete the following modules via the IGTT to ensure compliance with the role

1. Records Management and the NHS Code of Practice

2. Secure Transfers of Personal Data

3. Access to Information and Information sharing in the NHS

The Subject Access Lead should complete training every 3 years unless there is a significant change to legislation/guidance, in which case training should be brought forward.

ADDITIONAL TRAINING

It may be that none of the above specialist IG training is immediately applicable to your role. If you or your line manager feels that you require further IG training, please contact the Information Governance team for advice.

In addition to the specialist training outlined above, staff in identified roles such as IAO or IAA may wish to undertake further training utilising the NHS IGTT.

NETWORK AND CORPORATE SHARED DRIVE ACCESS

OBTAINING A NETWORK ACCOUNT

It is NHS policy that all staff should have access to email. To use email you require a network account. You also require an account to access the shared network drives.

If staff require an e-mail account or any changes to their IT set-up, they are required to fill in a SARC (System Access Request for Change) form on-line. This is accessed through "useful" links on the CCGs intranet, http://intranet.dudleyccg.nhs.uk/useful-links/Pages/Introduction.aspx

It is the user's responsibility to chase the IT Service to ensure that their network account is created in a timely manner. Please note that under no circumstances should another person's account be used in the interim if your account has not yet been set up.

It is the responsibility of line managers to notify the IT Service of changes in staff circumstances that may affect access to systems. These include job title, work location, maternity/sick leave. Managers should also notify the IT Service Desk of all leavers so that their network account can be disabled.

ACCESS TO INFORMATION

- Users will only be granted access to data and information that it is required as part of their job. Access is therefore granted on a 'need to know' basis.
- Access authorisation should be regularly reviewed, particularly when staff roles and responsibilities change.
- Staff must not access computer systems or data unless they have authority to do so. Access to files which are not in the course of the employee's duty will be considered a disciplinary offence. For example, accessing a friend or relative's, manual or electronic file. This may also be deemed a breach of the Computer Misuse Act 1990.
- Access should be requested via your line manager.

THIRD PARTY ACCESS TO CCG NETWORK

Third parties will not be given access to the organisations systems or networks unless they have formal authorisation to do so. All non-NHS companies will be required to sign security and confidentiality agreements with the organisation.

Third parties found accessing elements of the system they are not authorised to, will be deemed as causing a security breach and will be denied access immediately. An incident will be recorded following the CCGs incident reporting process and an investigation will take place to decide the outcome.

PREVENTION OF MISUSE

Any use of IM&T facilities for non-business or unauthorised uses without management approval will be regarded as inappropriate usage.

The Computer Misuse Act 1990 introduced three criminal offences. Staff must remember that the following offences can be enforced in a court of law:

- Unauthorised access
- Unauthorised access with intent to commit further serious offence
- Unauthorised modification of computer material

SOFTWARE LICENSING PROCEDURE

New software, which has not been properly developed and/or properly tested, is a threat to the security of existing data. All software and hardware procurements shall take account of the security requirements recommended by the IG team. Contravention of the recommendations may be considered a disciplinary offence.

UNAUTHORISED INSTALLATION OF SOFTWARE

Unauthorised software poses a risk to your computer, other computers and the network as a whole from malicious code embedded within the software. The risk applies to all programs and games downloaded from the Internet, on floppy disk, CD/DVD or any other storage media. Malicious code may be computer viruses and spyware, and the effects will vary depending on which has been downloaded.

A second and equally important reason why you should never use unauthorised software is because of licensing issues. The CCG is required to purchase licenses for the use of all software on its systems. If you install software without authorisation this process is by-passed and you put the organisation at risk of legal action from the owner of the software. If you are installing so-called free software it could be an illegal copy, or it could be trial software with an expiry date. Even if neither of these things apply, the software is likely to be for single personal use and require a license for corporate use.

INDIVIDUAL RESPONSIBILITIES

Individuals must not install software on to a CCG owned desktop or laptop computer and doing so constitutes a disciplinary offence. A request for installation should be made to the IT Service.

The IT Service audits all computer equipment including software. If unauthorised software is found on a system or if no license agreement has been purchased, IT Service staff are authorised to remove the software.

Should you suspect the presence of unauthorised software on your system you should report it to the IT Service, who can also advise on the procedure for purchasing software licenses.

It shall also be considered a disciplinary offence to connect any new hardware/ equipment to the network without prior approval.

EQUIPMENT DISPOSAL - REUSE OF SURPLUS EQUIPMENT WITHIN THE CCG

Departments should follow a general policy of internal cascading of any surplus equipment within their own area.

DISPOSAL OF EQUIPMENT

Once all information has been copied over to a new PC/disk, users must request that all hard disks and floppy disks of the old PC are destroyed by the IT Service.

This is to ensure that the CCG:

- Complies with obligations under European Environmental Legislation,
- Fulfils its commitment to the Waste Reduction Policy 1996 and Sustainability Policy 2000,
- Meets software license obligations and
- Reduces risk of sensitive data being released to unauthorised persons.

PASSWORD MANAGEMENT

Passwords are the front line of protection for user accounts. A lack of user responsibility towards IT systems password may result in the compromise of the organisations entire computer network and any national systems/applications accessed via the network.

All employees (including contractors and providers with access to the organisations computer systems) are responsible for taking the appropriate steps, to select and secure their passwords.

Login and passwords are granted based on the requirements of the post. Staff do not have inherent rights to access the organisations network or applications. **Any deviation from, or abuse of access privilege or rules contained in this section will be deemed a serious breach of policy. Formal disciplinary procedures may result.**

Please ensure that the following guidelines are followed to ensure appropriate password management:

- Sharing of logins and passwords is strictly forbidden.
- Passwords should consist of a mixture of upper and lower case.
- Passwords must not be written down and placed on view to others.
- Passwords need to be changed on a regular basis or if a password breach occurs.
- In the event of forgetting your password, please contact IT Services and they can then authorise a reset of your password should it be required.
- **Any member of staff who is either sharing their password or logging someone else onto the network with their user name is breaching the organisations policy and handbook and so may be subject to disciplinary action.**

INTERNET & INTRANET

PERMISSIBLE ACCESS

Access to the Internet is primarily for work or for professional development and training.

Reasonable personal use is permitted during your own time (for example, during your lunch break), provided that this does not interfere with the performance of your duties. Personal access to the Internet can be limited or denied by your manager. Staff must act in accordance with their manager's local guidelines. The organisation has the final decision on deciding what constitutes excessive use.

The internet must never be assumed to be secure. Confidential information or data must never be transmitted over the internet unless the data or information is encrypted. Information obtained through the Internet may not be accurate, and users must check the accuracy, adequacy or completeness of any such information.

NON-PERMISSIBLE ACCESS

No member of staff is permitted to access, display or download from internet sites that hold offensive material. To do so may constitute a serious breach of the organisations security and could result in dismissal and/or criminal prosecution. Offensive includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. Users must not create, store or distribute any material that is libellous, blasphemous or defamatory. This list is not exhaustive. Other than instances which demand criminal prosecution, the organisation is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet.

If a web page cannot be accessed it is possible that the site has been added to a ban list. Sites that are added to this list include ones that contain offensive content i.e. pornographic, terrorist, racist etc.

MONITORING

You should be aware that a range of monitoring is conducted on internet usage. This indicates time spent on the Internet and list of visited websites. Logs of internet usage are used to investigate allegations of misuse.

UNINTENTIONAL BREACHES OF SECURITY

If you unintentionally find yourself connected to a site that contains offensive material, you must disconnect from the site immediately and inform your line manager and the IT Service Desk.

It is a breach of security to download files which disable the network or which have the purpose of compromising the integrity and security of the organisations networks and/or file servers. To intentionally introduce files which cause damage to computers may result in prosecution under the Computer Misuse Act 1990.

ACCEPTABLE USE OF SOCIAL MEDIA & SOCIAL NETWORKS

NHS organisations of all types are now making increased use of social media and social networks to engage with their patients, other stakeholders, and to deliver key messages for good healthcare and patient services generally. These online digital interactions are encouraged and their use is likely to be further extended as new communications channels become available. Social media has great potential to help the NHS reach patients and service users that do not engage using traditional communications and engagement channels. However, the inappropriate or ill-considered use of social media also has the potential to damage both individual's and the NHS' reputation. It is therefore important that staff are aware that there are a number of legal implications associated with the inappropriate use of social media. Liability can arise under the laws of defamation, copyright, discrimination, contract, human rights, protection from harassment, criminal justice act etc. This list is however non-exhaustive.

Social media describes the online tools, websites and services that people use to share content, profiles, opinions, insights, experiences, perspectives and media itself. These tools include social networks, blogs, message boards, podcasts, microblogs, image sharing, social bookmarking, wikis, and vblogs.

The feature that all these tools, websites and services have in common is that they facilitate conversations and online interactions between groups of people.

Internal SharePoint sites also provide social networking capabilities and are included in this procedure.

It is important that all staff and contractors have a general awareness of the information risks and good practices associated with the protection of sensitive information in social media and other social interaction scenarios.

The organisation has the right to manage its reputation on all levels, including any employee interaction on social networking sites that could possibly reflect an opinion upon the organisation.

Personal use of social media at the workplace and at home

This section of the procedure provides guidance on the use of social media tools by NHS employees in a personal capacity. For example this includes a personal profile on Facebook or use of Twitter in a personal capacity by NHS employees.

It is important to remember that adherence to the expectations set out in this handbook applies equally whilst not at work as at work when any inference is made to work, either specifically or indirectly.

All policies apply equally inside and outside of work hours when work related.

Staff or contractors must be aware of their association with the organisation when using social media. If they identify themselves as an employee of a specific NHS organisation, they should ensure that their profile and any related content is consistent with how they would wish to present themselves with colleagues, patients and service users.

Staff or contractors who may not directly identify themselves as an NHS employee when using social media for personal purposes at home, should be aware that content they post on social media websites could still be construed as relevant to their employment at the organisation. For example, employees should not write or report on conversations, meetings or matters that are meant to be private or internal to the organisation.

Unauthorised disclosure of confidential information would constitute misconduct/gross-misconduct in accordance with the organisations disciplinary policy. Employees should not cite or reference patients, service users, partners or providers without their written approval.

The organisation will not accept liability for any actions arising out of employee's personal use of social networking sites.

Using social media for professional purposes

This section of the procedure relates to the use of social media tools by NHS employees in the course of carrying out their normal duties in delivering NHS services. For example this would include using a Facebook page to promote NHS activities and initiatives.

Setting up a unique social media presence for specific service / campaign

This can be used to:

- enhance engagement with a target audience. This is likely to work best for specific campaigns or issues (e.g. Quit smoking – through privileged access to content and information for ‘Facebook friends’; information re prize draw winners; uploading event photos, etc.)

- allow service users to share experiences (e.g. Quit smoking – people share tips on what’s helped them to stay cigarette-free)
- promote specific events via invites and newsfeeds
- drive traffic to the official website where more information is available
- send information/support directly to service users mobiles (e.g. via Twitter)

Interacting with existing external social media sites

This can be used to:

- engage with other service providers – creating a virtual network of relevant professionals to share and disseminate information and good practice and to act as a hub on relevant topics
- monitor what’s being said on-line about the organisation and its services, and give an authorised user the right-to-reply
- drive traffic to the organisation’s website and social media pages

Departments considering using Social Media

Managers may choose that using Social Media as means for communication as a benefit, however certain considerations must be made when scoping the use of Social Media.

- Moderating the site must be done on a 365 day basis, in order that any malicious or malevolent comments are removed as soon as possible. This must be undertaken within the department.
- Disclaimers on a social media sites does not remove the organisation’s obligations to accuracy and implications.
- Comments made to a social network site belonging to the organisation can be disclosed under the Freedom of Information Act 2000.
- When the organisation (or department within the organisation) creates a social network site such as Twitter or Facebook, the Information Commissioner has dictated that the organisation must be in a position to receive a Freedom of Information/Environmental Information Request via that medium and site.

Approval Process for access to Social Media

Any staff member wishing to set up a social media presence OR interact with existing external sites where they are identified as an organisation employee MUST follow the following procedure:

1. Obtain approval from relevant Line Manager and Director

2. For communications on behalf of the organisation, any other NHS services, or a partnership of which the organisation is a member, a business case should be made to the CCGs management team who will consider and refer to directors with their recommendations. The Information Governance, Human Resources and Communications team should be consulted during this process.

3. For staff or contractors wishing to use an NHS or other professional websites or social media tool during working hours to share best practice or seek advice and feedback from other colleagues as part of their role, they should gain the appropriate authorisation from their line manager before proceeding. Line managers unsure of which sites, forums or tools are acceptable for use should speak to the Information Governance team for advice.

General usage guidance

When using social media, employees should respect their audience. As a general rule, employees should be mindful of any detrimental comments made about colleagues whilst using social media. Any conduct which breaches the employee code of conduct such as failing to show dignity at work (harassment), discriminatory language, personal insults, obscenity, and disclosure of confidential information will be considered a disciplinary matter. These examples are not exhaustive.

Staff and contractors should also show proper consideration for others' privacy and for topics that may be considered sensitive or controversial.

Staff and contractors are encouraged not to divulge who their employers are within their personal profile page (e.g. in accordance with RCN guidelines, "RCN Legal Advice on using the internet"). However, those that do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity.

Staff and contractors must not share details of the organisation's implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security.

Staff and contractors are ultimately responsible for their own online behaviour. They must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassment, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution. Remember; once something is put on a social networking site even if you delete it, there may be a record of it kept indefinitely.

Note: These guidelines apply to all methods of accessing social networks. This includes organisation-owned or personal computers, Smartphones, iPads, etc.

EMAIL

EMAIL RETENTION

There is occasionally a misconception that email messages constitute a short-lived form of communication. All email messages are subject to Data Protection and Freedom of Information legislation and can form part of the corporate record. Emails should therefore be retained according to the subject of the message in line with the NHS Records Management Code of Practice retention schedule.

Be mindful when deleting emails permanently, as under the Freedom of Information Act 2000, you may need to refer back to such communications or provide as evidence in responding to FOI requests.

The Data Protection Act 1998 gives individuals the right to access any information held about them, including email messages. In addition, Courts and Employment Tribunals have the power to order disclosure of emails that may be relevant to a case.

For a permanent record, emails should be saved to an appropriate location on the shared drive.

DOS AND DON'TS OF EMAIL

Users may not use the organisations email systems:

- To breach copyright or intellectual property rights of a third party.
- To view, store, download, send, forward or copy inappropriate material. Examples include but are not limited to; obscene or pornographic material, discriminatory material or anything of a criminal nature.
- To send defamatory or libellous messages.
- To breach the Data Protection Act 1998.
- To forward chain or junk email.

In addition, the use of a non NHS email account (personal or web mail) is not permitted for the purpose of the organisations business.

Personal use of the CSU email system is not permitted where it substitutes for a webmail system such as gmail.

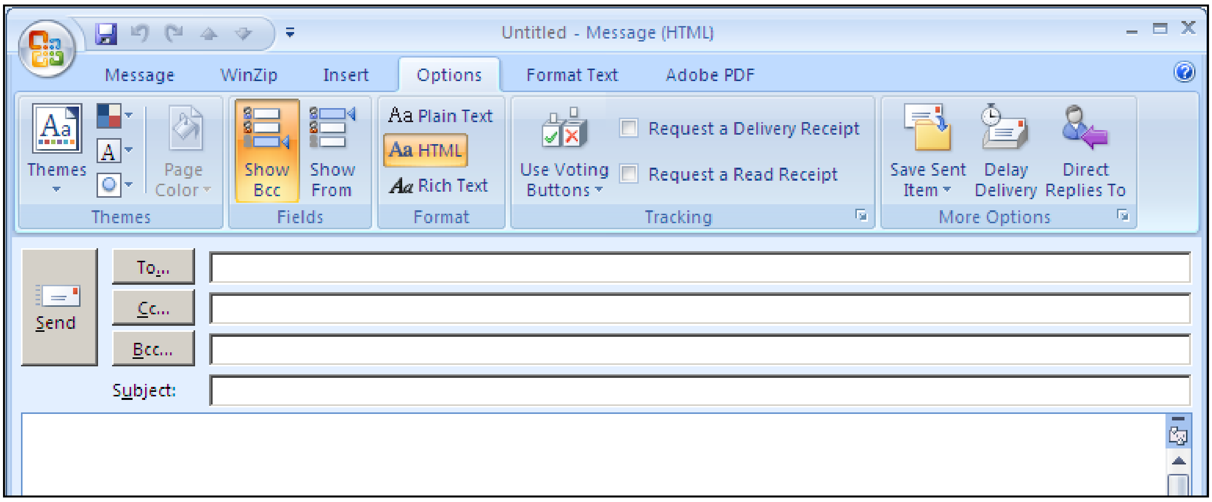
The organisation considers email as an important means of communication and recognises the importance of appropriate email content and prompt replies in conveying a professional image and delivering good customer service.

The organisation requires users to adhere to the following guidelines:

- Write well-structured e-mails;
- Use short, descriptive subjects;
- Signatures must adhere to the corporate standard;
- Do not send unnecessary attachments;
- Ensure that the purpose and content of the e-mail message is clearly explained;
- Do not write emails in capitals. This can be considered rude and aggressive;
- Use a spell checker before emails are sent;
- If you require a response by a particular date, let the recipient know this;
- Only mark emails as important if they really are important;
- Ensure emails are only sent to people who need to see them;
- Email should be treated like any other correspondence and should be answered as quickly as possible;
- When on annual leave or away from the office for over one day, the Out of Office facility should be used;
- Ensure that the content is verifiable, evidence based and capable of being subjected to public scrutiny, including applications made under the Freedom of Information Act 2000;
- Be responsible about your use of email; be aware that the email you send may be forwarded without your prior knowledge or consent, or you may be sending to a recipient who has shared access to their inbox with another member of staff, for example their PA;
- Make a clear distinction between opinion and fact.

SENDING EMAILS TO MAILING/DISTRIBUTION LISTS

If an email is to be sent to a number of people or to the members of a mailing/distribution list, it may be that the recipients do not (or should not) know who else the email has been sent to, particularly if the recipients include members of the public. Therefore the “BCC” field should be used rather than the “To” field as this allows the email addresses of the other recipients to be concealed.



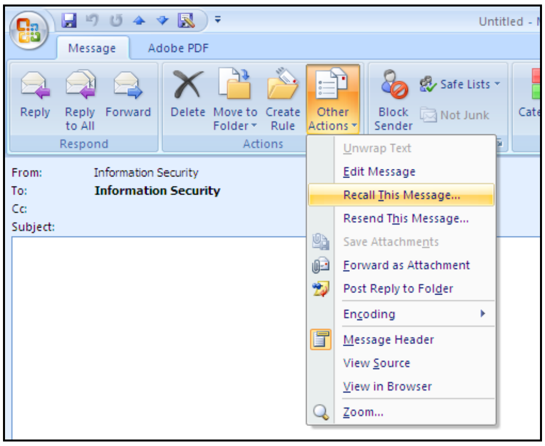
This means that the recipient list of the email cannot be reused and it reduces the chances that the recipients will receive spam or viruses as a result of having shared their email address with many others.

Alternatively, it may be advisable to set up a distribution list and use the alias rather than including individual names or email addresses in the headers.

RECALLING EMAILS

If an email has been sent in error, for example to an incorrect recipient or an attachment has been missed off, it is possible to recall the email.

To do this, open the sent email that is to be recalled and select “Recall This Message” from the “Actions” menu. You will then have the option to either delete the message or replace it with a new one.



From: Information Security
To: **Information Security**
Cc:
Subject:

Please note that messages must be recalled as soon as possible because this function will not work if the recipient has already read the email. Also, the recipient of the email that you want to recall must also be using an Exchange account, not a webmail account such as gmail.

MONITORING

At the request of the Managing Director the IT service may carry out investigations into email usage.

All external emails are routinely virus scanned and where viruses are detected the email is quarantined until clean. If this is impossible then the email administrator will contact the recipient.

In this case the email would be opened by the recipient within the quarantined area.

Formal complaints about the misuse of email will be investigated and managed according to the organisations existing grievance and disciplinary policies. Inappropriate emails will be automatically blocked for the protection of the organisation and individuals (e.g. spam and adult content)

Legislation came into force in October 2000 providing circumstances in which the organisation can lawfully intercept emails made on its own systems such as:

- Gaining routine access to business communications;
- Monitoring standards or service and training;
- Preventing or investigating crime;
- Unauthorised use of systems.

Any use of email that breaches this procedure will be investigated and may result in the matter being treated as a disciplinary offence under the organisations disciplinary procedure.

LONG TERM ABSENCE

If a staff member is on long term absence (more than four weeks), their line manager should, with the help of the IT Service, redirect their email account to someone else within the department who has authority to manage that account. The justification of redirecting the messages should be clearly established prior to redirection. The duty of confidentiality should be impressed upon the member of staff who receives the redirected mail.

It must also be ensured that an out of office message is added to the account at the earliest opportunity. It is recommended that it is set up so that an automated response is sent to every email, rather than just the initial email received from a sender.

SHARED EMAIL ACCESS

There may be circumstances where there is a requirement, for example, for a PA to access a Director's email account.

Under no circumstances should this be facilitated by the Director sharing their network account password with their PA. Doing so is a breach of CCG policy and must be reported as an incident via the CCGs incident reporting process.

Microsoft Outlook provides the facility for a user to share their inbox with other users in the same way as a calendar can be shared. Other items such as contacts or tasks can also be shared in this way.

It should be noted that where access is granted to another user, that user may have access to any private, confidential or sensitive materials associated with the respective user account. As a result, access should ONLY be authorised where this is absolutely necessary for operational purposes (and preferably with the individual's consent). Access can be "tailored" by applying rules within your inbox. For example, a rule could be set up which moves any items received which are marked as confidential to a subfolder rather than leaving them in your main inbox.

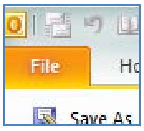
Any person, who is granted access to another user's inbox to fulfil the requirements of their role, should only view the information required to allow them to do so. Users accessing inboxes of other staff are required to treat all material viewed as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. They must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters.

If you need to share your complete inbox, including any sub folders, with another user then this needs to be facilitated by the IT Service and so a call must be logged with your IT Helpdesk. When doing so, please be mindful that this will mean that ALL emails will therefore be accessible to the user with whom you share your inbox.

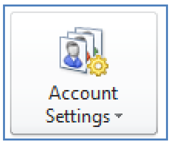
HOW TO SHARE YOUR INBOX (BASED ON MICROSOFT OUTLOOK 2010):

If you just wish to share your main inbox (and not sub folders) then you can facilitate this yourself by following these steps:

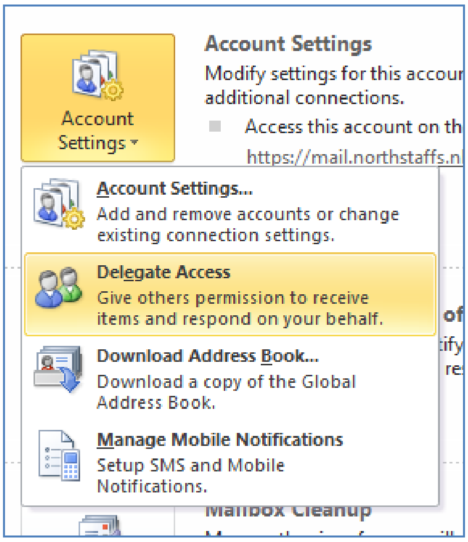
From the File menu in Outlook:



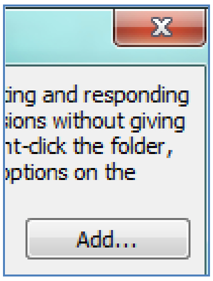
Click on Account Settings:



and then Delegate Access:

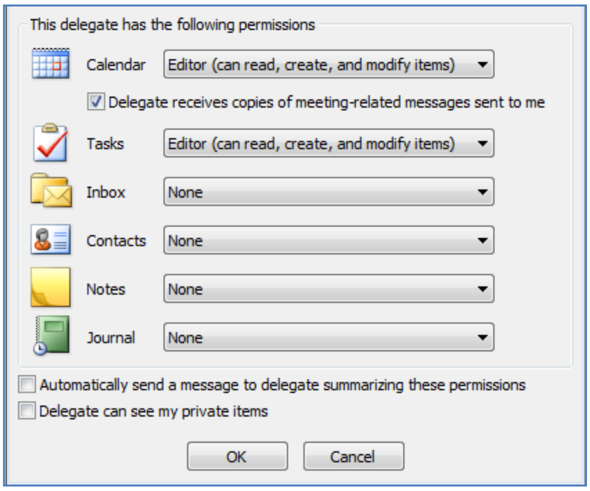

Account Settings
Account Settings
Modify settings for this accour
additional connections.
Access this account on th
https://mail.northstaffs.n
Account Settings...
Add and remove accounts or change existing connection settings.
Delegate Access
Give others permission to receive items and respond on your behalf.
Download Address Book...
Download a copy of the Global Address Book.
Manage Mobile Notifications
Setup SMS and Mobile Notifications.
Mailbox Cleanup

Click on Add:



Find the person with whom you wish to share your inbox in the global address list that appears then double click on their name.

The following pop up will then appear:



This delegate has the following permissions

Calendar	Editor (can read, create, and modify items)
	☑ Delegate receives copies of meeting-related messages sent to me
Tasks	Editor (can read, create, and modify items)
Inbox	None
Contacts	None
Notes	None
Journal	None

☐ Automatically send a message to delegate summarizing these permissions

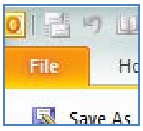
☐ Delegate can see my private items

Use the drop down lists and check boxes to set the access permissions you require and then click on OK.

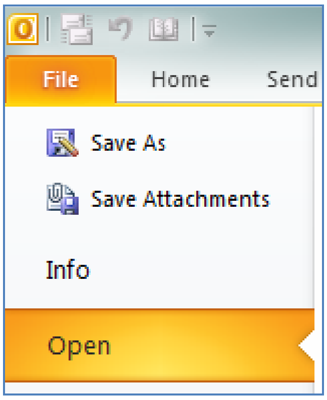
You will then be able to see the person you have just added in your list of delegates.

HOW TO ACCESS AN INBOX WHICH HAS BEEN SHARED WITH YOU (BASED ON MICROSOFT OUTLOOK 2010):

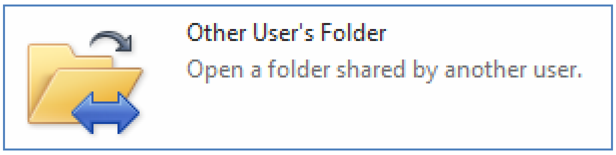
From the File menu in Outlook:



Click on “Open” on the left hand side of the screen:



Click on “Other User’s Folder”:



In the pop up that appears, click on “Name”. This will open the global address list. Find the name of the person who has shared their inbox with you and double click on it.

Click on OK.

The other user’s inbox will then be opened.

If IT have facilitated your access to another users full inbox (including subfolders) then the inbox should be displayed as a folder in the left hand side of your Outlook.

ACCESSING ANOTHER USERS INBOX VIA THE IT SERVICE

If it is not possible or appropriate to request a user share their inbox with you, for example because they are absent from work, have left the organisation or the access is required for a HR investigation, then a request must be made to the IT Service using the form provided in Appendix C.

CLEAR SCREEN & CLEAR DESK

Clear Screen

- Laptops and PCs should be locked when they are not in use regardless of how long the computer will be left unattended (i.e. to go to the toilet or to speak to a colleague at their desk, etc.). This can be completed by pressing **Ctrl** – **Alt** – **Delete** and then **ENTER** or holding the windows key and pressing L.
- On the occasions when there is a genuine mistake and screens are not locked, the password protected screensaver will launch after15 minutes idle time. This should however only be used as a 'back up' for when the screen is not locked.
- You should always shut down your computer when leaving the office for the day. This enables any security and system updates to be rolled out and installed when the computer is restarted.
- Organisation computers should not be left logged on when they are not in use as this stops others being able to use the computer when you are out of the office.
- Computer screens should always be angled away from the view of unauthorised persons, in particular when working from a reception desk or ground floor office.

Clear Desk

- Where practically possible all confidential papers and removable media, including laptops etc. should be stored in suitable locked cabinets or other forms of security furniture when they are not in use, especially outside of working hours.
- Staff who are required to attend meetings or leave their desks unoccupied for more than one hour at a time, are expected to remove any confidential information from their desks.
- Where lockable filing cabinets, drawers, cupboards etc. are not available, office/room doors must be locked if left unattended. At the end of each day all sensitive information should be removed from the workplace and stored in a locked area. This includes all person identifiable information, as well as business critical information such as salaries and contracts.
- Staff should also be aware that information left on desks is more likely to be damaged or destroyed in a disaster such as fire, flood, etc.
- Any visitor, appointment or message books should be stored in a locked area when they are not in use.

SAFE HAVEN PROCEDURES - SENDING PERSON CONFIDENTIAL DATA

If person confidential data (PCD) needs to be sent inside or outside of the organisation by post or fax, the Safe Haven procedures outlined in this document must be followed.

Safe Haven is a term used to describe either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure person confidential data (PCD) is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by post, fax or other means.

Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

Before sending any PCD, it should be considered whether it would be sufficient to send anonymised or pseudonymised information instead.

SAFE

It is secure to send emails containing PCD within the CCG, ensuring that you confirm the email address of the person you are sending the email to and request confirmation of the receipt of the email. When sending emails containing PCD outside the CCG, Dudley CCG currently use encryption Sophos.

SAFE HAVEN POST PROCEDURES

Important points to note when sending PCD by post:

- PCD should **never** be sent in internal envelopes.
- PCD should **never** be sent in previously used envelopes.
- PCD, whether being sent internally or externally, must always be tracked.

This can be done by using either a tracking system or post book. The following information must be included as a minimum:

- Date the information is being sent
- Method of sending, i.e. internal, recorded delivery, 1st class, etc.
- What information is being sent
- Where the information is being sent to
- Initials of the person responsible for sending the information.
- Request that the recipient confirms receipt.

INTERNAL POST PROCEDURES

When sending PCD in the internal post system the following procedures need to be followed at all times:

Secure Bag**:

- ✓ Log all items which are being sent, stating where it is going to, date sent; secure bag number and the signature of the person packaging the information.
- ✓ Ensure that the secure bag is numbered and the information is placed inside along with a compliments slip or memo, requesting that the recipient calls to confirm receipt.
- ✓ Seal the bag, using an appropriate seal.
- ✓ Place into the internal mail ready for sending.
- ✓ Request that the recipient confirms receipt.

**Secure bags are the recommended way to send PCD in the internal mail. The secure bags are far more cost effective than standard envelopes and every effort should be made to use this method.

Standard Envelope:

- ✓ Log all items which are being sent, stating where it is going to, date sent, and the signature of the person packaging the information.
- ✓ Place in a new envelope and mark clearly **"Private and Confidential"**.
- ✓ Seal the envelope and place sellotape over the seal. Sign or initial diagonally over the sellotape so that the writing can be seen either side of the tape was it to be removed.
- ✓ Request that the recipient confirms receipt of the letter, either by enclosing a compliments slip or covering note.

EXTERNAL POST PROCEDURES

When sending PCD in the external post, the following procedures need to be followed at all times:

Tamperproof Envelopes (Person Confidential & Commercially Sensitive)

- ✓ If information being sent out contains **any** identifiers then it should always be sent in a tamperproof envelope.
- ✓ Information which is commercial in confidence should always be sent in a tamperproof envelope.

- ✓ Consider whether a secure method for sending confidential information through the external post is required e.g. recorded delivery.

Standard Envelopes (Appointment Letters, etc.)

- ✓ Ensure that the full address is used and visible.
- ✓ Mark clearly on the front of the envelope “**Private & Confidential”.**
- ✓ Ensure that the envelope is sealed appropriately. If the envelope does not seal sufficiently, use sticky tape to ensure that the letter will not open in transit.
- ✓ Complete the post book stating what has been sent, where, when, by who and method of delivery.

SAFE HAVEN FAX PROCEDURES

When sending PCD by fax, the following procedures need to be adhered to at all times:

- Contact the recipient to notify them that you are sending a confidential fax and double check the fax number.
- Ask the recipient to confirm receipt of the fax by return telephone call.
- Always use a fax cover sheet and make sure your fax cover sheet states who the information is for, the number of pages being sent and mark it “Private and Confidential”.
- Where possible, personal details (e.g. names and addresses) should be faxed separately from clinical details. Both faxes must be accompanied by the NHS number to allow them to be linked.
- The fax machine should be locked using a pin number, which is only available to staff who are authorised to access the Safe Haven.
- The fax machine should be switched off outside of working hours, to ensure faxes are not received when there is nobody available to collect them.
- Where possible, speed dials should be used when sending faxes. A list of all programmed speed dials should be kept with the fax machine, and this list must be kept accurate and current.

Please contact the Information Governance team for advice on whether a fax can be designated as a Safe Haven.

SAFE HAVEN TELEPHONE PROCEDURES

When sharing PCD over the telephone, the following procedures need to be adhered to at all times:

When receiving calls requesting personal information:

- ✓ Verify the identity of the caller
- ✓ Ask the reason for the request
- ✓ Ensure that the caller is entitled to the information that they are requesting – if in doubt, take advice from your manager or the Information Governance Team.
- ✓ If speaking to a service user, ask questions that require them to provide information, rather than giving them details which they need to confirm, e.g. ask them for their address, rather than telling them what is on their record and asking if it is correct.
- ✓ If you need to pause the call for any reason, remember to use "hold" to ensure the caller can't overhear other confidential conversations that may be going on in the background.
- ✓ Call back to the main switchboard and ask to be put through. Do not call back to direct numbers or mobile phones.
- ✓ Ensure that you cannot be overheard when providing personal information.
- ✓ Always be sure to leave the minimal information on answer machines when leaving messages, don't leave any person identifiable information.

SAFE HAVEN ROOM REQUIREMENTS

If confidential information is to be received in a specific location:

- It should be to a room/area that is lockable or accessible via a coded key pad known only to authorised staff.
- The room/area should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to all members of staff working in the same building or office, or to visitors.
- If the room/area is on the ground floor any windows should have locks on them.
- The room/area should conform to health and safety requirements in terms of fire, flood, theft or environmental damage.
- Manual paper records containing personal information should be stored in locked cabinets when not in use.
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use.
- Equipment such as fax machines should have a code password and be turned off out of office hours, (if possible).

Please contact the Information Governance team for advice on whether a room can be designated as a Safe Haven.

SAFE HAVEN ROOM PROCEDURES

- A list of staff authorised to enter the Safe Haven room must be maintained. Those staff listed will need to be authorised by the Caldicott Guardian for the organisation.
- Only staff named on the above list should be provided with either, the key code, swipe card or key to the Safe Haven room.
- No-one who is not listed should be provided with access to the Safe Haven room, under any circumstances.
- Should anyone be required to have access to the room for either data quality or audit purposes etc., those people should also be approved and included on the list of authorised staff.
- The door to the Safe Haven room should be kept locked at all times, even when the room is in use.
- No person identifiable information should be left in trays or on desks when not in use and should be locked away in suitable storage.
- Any computers within the Safe Haven room should be positioned facing away from the door or any windows. Computer screens should be locked immediately and not wait until the screensaver appears.

PROCESSING/SENDING PCD OUTSIDE THE EUROPEAN ECONOMIC AREA

The eighth principle of the Data Protection Act (1998) states that:

“Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

If you need to send PCD in any format to countries outside of the EEA you must discuss this with the Information Governance team as the levels of protection for the information may not be as comprehensive as those in the UK. You may also need to check with software suppliers to ensure that their servers are located within the UK or EEA and that they conduct any development and bug fixes etc. within the UK or EEA.

INFORMATION RISK ASSESSMENT AND MANAGEMENT PROGRAMME

Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the CCG.

There needs to be a comprehensive programme of activity across the CCG to identify information risks and manage them effectively. From the outset this needs to be recognised as an ongoing activity. A number of key activities in the Information Governance toolkit form the basis of building an information risk framework, namely:

- Mapping flows of information
- Identifying and maintaining a register of key information assets
- Setting out continuity plans for periods of information unavailability

MANAGING INFORMATION ASSETS

Information assets are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation, such as:

- Databases
- data files
- contracts and agreements
- system documentation
- research information
- user manuals
- training materials
- operational/support procedures
- business continuity plans
- back up plans
- audit trails
- archived information

**Please note that this list is not exhaustive.*

Information assets could be kept in a variety of formats and on a variety of media, e.g. paper, on a shared drive (e.g. the n drive), on removable media (e.g. USB memory sticks, CD-ROM).

Examples of paper assets include:

- patient records
- personnel files
- letters

Examples of electronic assets include:

- spreadsheets
- annual leave/sickness records
- local databases

- referrals
- annual leave sheets
- sickness absence returns
- expenses
- papers for meetings
- scanned documents
- electronic copies of letters

Information assets may contain **person identifiable** or **commercially sensitive** information.

A template has been developed which, with the support of the CSU Information Governance team, will allow Information Asset Administrators (IAAs) and Information Asset Owners (IAOs) to identify information assets and record details of their content, the security arrangements in place to protect them, and what business continuity arrangements are in place. For each question, a specified range of answers are provided. This approach will allow the information assets to be risk assessed using a standard risk scoring matrix to ensure consistency of risk assessments across the CCG.

Further to this, IAOs are required to assess the worst case scenario of the possible effects the loss of confidentiality, integrity and availability of each information asset would have to the business, including financial, adverse publicity, relationship with patients or NHS and the risks associated with non-compliance with legislation. This process will assess the business criticality of the asset to allow the CCGs critical assets to be identified, providing the basis of this component of departmental and organisational business continuity plans.

All organisations are subject to change brought about by modifications to the operational and technical environments. These in turn change the information assets held by the organisation and the risks associated with them, resulting in a requirement to review any previously recorded information assets and risk assessments. Consequently, the information asset register should be subject to regular maintenance by IAOs and IAAs, with formal review conducted at least annually. It is essential that whenever new information assets are created, the relevant IAA or IAO is informed, to allow them to create an entry in the Information Asset Register.

This formal review of assets and risk assessments will be conducted at least annually.

PERSON IDENTIFIABLE DATA FLOW MAPPING

In the NHS, numerous urgent and routine transfers of person confidential data (PCD) take place each day. It has long been recognised that this information is more vulnerable to loss or compromise when outside the organisation, i.e. being carried around or sent/copied from one location to another. The requirement to map information flows has been included in organisational confidentiality audits since 2008/09 (version 6 of the IG toolkit).

To ensure all transfers are identified, the organisation must determine where, why, how and with whom it exchanges information. This is known as Data Flow Mapping and the comprehensive register provided by this exercise identifies the higher risk areas of information transfers requiring effective management. It also allows any Information Sharing Agreements or contracts that should be in place to be identified.

To adequately protect transfers/flows of information, the organisation must identify the transfers, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all information (including personal information) must comply with the organisations Safe Haven Procedures and relevant legislation (e.g. Principle 7 of the Data Protection Act 1998 which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage to, personal data).

The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence. With effect from April 2010 fines of up to £500,000 may be imposed by the Information Commissioner's Office on organisations and individuals within organisations that do not take reasonable steps to avoid the most serious breaches of the Data Protection Act.

The information recorded in the Information Asset Register allows the identification of all assets of which part or all of their content are sent or received either internally or externally to the organisation. For those assets which are identified as moving in this way, a further template is completed by the IAA so further information is collected about how and where the information is transferred. This information is then risk assessed to identify areas of high risk and any areas of non-compliance with the CCGs safe haven procedures.

As with the Information Asset Register, person confidential information flows are subject to change and should therefore be reviewed regularly. A formal review will be conducted annually.

INFORMATION SHARING

Whenever person confidential data (PCD) is shared, the sharing must be fair, transparent and in line with the rights and expectations of the people whose information is being shared.

Sharing can take the form of:

- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties;
- exceptional, one-off disclosures of data in unexpected or emergency situations; or
- different parts of the same organisation making data available to each other.

If you are unsure what constitutes personal data, please contact the Information Governance team for guidance.

If a request is made for PCD to be shared, the first thing to be considered must always be whether data actually needs to be shared in an identifiable form. Could the same purpose be met by using either anonymised or pseudonymised data?

It is important that in every instance where PCD is to be shared, a legal basis for the sharing is established. This could be one of the following:

1. The data is to be shared to enable direct care (must be able to evidence a medical intervention for the patient at the end of the process)

2. Explicit consent from the individual about whom the data to be shared

3. Statutory obligation, e.g. a court order

4. Legislation, e.g. Children's Act 2004, Mental Capacity Act 2005

5. The receiver holds a section 251 approval which allows them to collect PCD without requiring any further consent

Once this legal basis has been identified, the sharing must be documented in some way. At its simplest, for example for a direct care purpose or for a statutory obligation, this could be by making a note in the file being shared. However, in most cases a formal agreement should be put in place.

There are 3 types of agreements to be considered:

Information Sharing Agreement	For use when sharing PCD with any other party who will use the information for its own purpose.
Data Processor Agreement	For use when sharing PCD with any other party who will process the data on the organisations behalf and then return the data to the organisation without using it for their own purpose.
Contracts	Whenever information is to be shared with any other party it is preferable for a contract to be put in place which includes adequate IG clauses to govern their use of any information that is shared with them, **whether it is PCD or not**.

The CCG must consider how its role as a commissioner of services sometimes necessitates the sharing of PCD as part of a service, although the CCG itself may not be a party to the data sharing. In such circumstances, the CCG has a responsibility to work with the data controller(s) to ensure that appropriate agreements are put in place.

The Information Governance team can advise on which type of agreement is required and will review any proposed sharing agreements against a checklist to ensure that they cover all requirements.

PRIVACY IMPACT ASSESSMENTS

All new projects, processes and systems (including software and hardware) which are introduced must comply with confidentiality, privacy and data protection requirements. Privacy impact assessments (PIAs) are a tool which can help the CCG identify the most effective way to comply with these requirements and to fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach and should be used throughout the development and implementation of a project, using existing project management processes.

Although not a legal requirement, within the NHS the use of PIAs is mandated through its inclusion as a requirement set out in the Information Governance Toolkit (Req. 237).

The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

These can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy.

PIAs are concerned primarily with informational privacy which can be defined as:

the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

The process of conducting a PIA should begin early in the project. When it becomes clear that a project will have some impact on privacy an organisation should start to consider how they will approach this. This does not mean that a formal PIA must be started and finished before a project can progress further. The PIA should run alongside the project development process. What begins as a more informal early consideration of privacy issues can be developed into part of the PIA.

Projects which might require a PIA

The core principles of PIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals. PIA terminology often refers to a project as the subject of a PIA and this should be widely construed. A PIA is suitable for a variety of situations:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

The first stage in identifying whether there is a need for a PIA is to complete a screening checklist, the results of which will then identify if further information and a PIA is required. The PIA Checklist and Questionnaire can be found in Appendices E and F of this handbook.

CONFIDENTIALITY AND DATA PROTECTION

The collection and use of person confidential data (PCD) is governed by the principles of the Data Protection Act 1998 and, in the case of information pertaining to patients or service users, also the principles arising from the Caldicott Committee (1997 Caldicott Report) and subsequent Information Governance Review in April 2013 (known as Caldicott 2).

All employees are bound by a legal duty of confidence to protect PCD they may come into contact with during the course of their work.

All employees are responsible for maintaining the confidentiality of information gained during their employment by the organisation. This also extends after they have left the employ of the organisation.

This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and, in addition, for health and other professionals through their own professions' Code(s) of Conduct.

This means that employees are obliged to keep any PCD strictly confidential. It should be noted that non-person identifiable information that may be classed as **commercial in confidence** should also be treated with the same degree of care as PCD.

No employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the organisation's security systems or controls in order to do so.

Definitions

Confidential Information can be anything that relates to patients, staff, their family or friends, or the business of the member organisations, however stored.

For example, information may be held on paper, computer files or printouts, video, photograph or even heard by word of mouth. They may also be stored on portable devices such as laptops, palmtops, USB pens, mobile phones, digital cameras and CDs.

It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any company confidential information.

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, surname, address, postcode, date of birth, NHS number, National Insurance number etc.

Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information as defined by the Data Protection Act 1998 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Gender Identity
- Trade union membership
- Physical or mental health or condition
- Sexual orientation
- Commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

For this type of information even more stringent measures must be employed to ensure that data remains secure. During your work you should consider all personal information to be sensitive. The same standards should be applied to all personal information you come into contact with.

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances unless they are directly involved in their medical care or with the employees administration on behalf of the organisation. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

Do not talk about patients/clients in public places or where you can be overheard by the public, patients/clients or even other members of staff.

Contracts of Employment

All staff contracts of employment include data protection and confidentiality clauses. Agency and contract staff must also sign confidentiality clauses before commencing work in the organisation.

Providing advice and responding to individuals about the use of their information

The organisation will inform individuals if their information is to be used for another purpose or disclosed to a person or organisation that the individuals would not have anticipated.

The Data Protection Act gives the 'subject' the right to contact the organisation about a number of issues relating to use of their personal information, this may include:

- Objections to how their personal information is processed
- Requests for certain possible disclosures of their information to be restricted
- Requests for detailed information about how their information is used by the organisation

Advice must be sought from the Caldicott Guardian and/or the CSU Information Governance Team to ensure satisfactory responses and actions are taken.

Significant proposed changes in the use of personal information may require the completion of a Privacy Impact Assessment (PIA).

CONFIDENTIALITY AUDITS

Introduction

All CCGs should already have control mechanisms in place to manage and safeguard confidentiality, including mechanisms for reporting incidents. The Information Governance toolkit also requires that documented procedures are implemented to ensure these controls are monitored and audited.

Organisations should have processes to highlight actual or potential confidentiality breaches in their systems, particularly where personal confidential data (PCD) is held. They should also have procedures in place to evaluate the effectiveness of the controls within the systems.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented may result in a breach of that confidentiality, therefore contravening the requirements of the Caldicott Reports, the Data Protection Act, the Human Rights Act and the Common Law duty of Confidentiality.

Scope

All work areas within the CCG which process (handle) confidential information will be subject to this confidentiality audit procedure. These work areas have been identified through population of the Information Asset Register and Data Flow Mapping tool. Confidentiality audits will focus on controls within electronic systems. Hard copy records will be the subject of separate Information Security Audits to examine the physical security measures in place to prevent their unauthorised access.

Objectives

- To establish an approach to monitor access to confidential information within the CCG.
- To provide assurance that the necessary controls are in place for accessing confidential information.
- To discover whether confidentiality may be breached or put at risk through misuse of systems, or as a result of poorly applied controls.

Monitoring and Auditing Access to Confidential Information

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis.

Confidentiality audits will focus on controls within electronic records management systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of weak, non-existent or poorly applied controls.

Actual or potential breaches of confidentiality should be reported as incidents, in order that action can be taken to prevent further breaches taking place.

The Information Security Officer will work with System Owners to ensure that audits of systems and access controls are conducted in order to provide an assurance that the controls in place are working effectively.

Audits will check:

- Failed attempts to access confidential information;
- Repeated attempts to access confidential information;
- Access of confidential information by unauthorised persons;
- Evidence of shared login sessions/passwords;
- Previous confidentiality incidents and actions arising from such incidents;
- Appropriate use of smartcards;
- Appropriate allocation of access rights to systems which contain confidential information;

Audit methods and facilities to be utilised

- Audit reports generated from systems identified as being within the scope of this audit;
- IT Service reports regarding central IT systems;
- Registration Authority (smartcard usage) enhanced reporting facilities;
- Investigation of reported incidents reports;
- Monitoring of Caldicott log.

Monitoring access to confidential or business sensitive information

All staff should be aware that electronic systems that access, process or transfer personal sensitive information are monitored on a continuous basis. Any breach of security or infringement of confidentiality may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with the CCGs disciplinary procedures. In addition, unauthorised disclosure of personal information is an offence and could lead to prosecution of individuals and/or the organisation.

Reporting

Once the audit has been completed a formal report should be produced detailing the outcome of the audit. It will include a summary of the findings of the audit, together with observations of non-compliance and recommendations which have been made.

Where non-compliance is observed, this should be recorded as soon as possible, be sufficiently detailed, including all the facts and referring to any relevant evidence. The detail recorded should include an outline of what was observed, where it was observed, who was involved, the date of the observation and why it was considered non-compliant. Each non-compliance observed will be referenced to the section of the relevant CCG Policy or handbook to highlight where there may be an issue with the implementation of a procedure that the CCG has approved, and will have an associated recommendation which should be discussed and agreed with the head of department and other staff as appropriate. Each recommendation will also include a target date for completion and a named individual who will be responsible for ensuring that the recommendation is implemented.

Non-compliance can fall into one of two categories:

Major Non-compliance: this would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequences.

Minor Non-compliance: these could include one-off occurrences of non-compliance; there are likely to be only minor consequences.

Where a number of minor instances of non-compliance are observed in the same functional area or department, this may indicate a more serious problem within that area. If this is the case, these instances of non-compliance should be combined into a Major non-compliance.

Audit Follow-Up

Reports on audit outcomes including progress on recommendations made will be considered by the Information Governance Group who will monitor progress on actions identified.

Audit Closure

Once corrective action has been checked and agreed as compliant by the auditor, the audit can be formally closed.

INFORMATION SECURITY AUDITS AND SPOT CHECKS

Introduction

It is essential that all staff comply with the procedures put in place by the CCG to ensure information security. This helps minimise the potential risks to themselves and others, as well as reducing the financial costs arising from the loss of data, equipment and personal possessions.

Potential security issues and risks should be identified and mitigated by implementing effective controls and solutions. The CCGs main security objectives are:

- The protection of property against fraud, theft and malicious damage.
- The protection of all records and personal information, regardless of how these are held (electronic or paper records).
- The smooth and uninterrupted delivery of services.

In practice, this is applied through three cornerstones - Confidentiality, Integrity and Availability

- Information must be secured against unauthorised access – Confidentiality
- Information must be safeguarded against unauthorised modification – Integrity
- Information must be accessible to authorised users at times when they require it – Availability

Scope

All work areas within the CCG will be subject to Information Security audits and spot checks. The security measures of each building and office will be reviewed and their implementation will be tested. General working practices will be inspected through observations and interviews to ensure compliance with the security procedures and Information Governance guidelines.

Objectives

- To establish an approach to monitor the security of the CCGs Information Assets and physical assets such as IT equipment.
- To provide assurance that the necessary controls are in place to maintain the security of the CCGs Information Assets and physical assets.
- To identify areas where confidentiality or security procedures may be breached and assets put at risk as a result of poorly applied controls.

Information Security Spot Checks

Information Security Spot Checks will be unscheduled checks by the CCGs Information Governance Support Officer and/or Information Security Officer to review compliance with the CCGs procedures and whether staff are adhering to them in their day to day working.

The checks will consider:

- Physical security provisions of the building and offices
- Security applied to manual files e.g. storage in locked cabinets/locked rooms
- IT Security Processes e.g. screens locked when not in use
- Security of IT equipment and portable media when not in use
- Security of post handling areas
- Security of confidential fax handling
- Clear desk policy
- Clear screen policy
- Security of offsite storage boxes prior to removal to storage
- Evidence of secure waste disposal
- Use of whiteboards for confidential information

The spot checks will take place during the working day and early morning/late evening to provide a view of compliance both inside and outside of working hours. The focus of the checks may therefore vary dependent upon the time of the audit as some aspects, such as clear screen, may not be applicable outside of working hours.

Information Security Audits

In addition to the Information Security Spot Checks, audits will be carried out which, rather than being a general appraisal of compliance, will focus on specific information assets to verify and test the security measures specified as being in place in the assets entry in the Information Asset Register, including the methods of transmission for any associated data flows where possible (for example examination of emails to ensure they are encrypted would be beyond the scope of the audit). The audit would also consider arrangements for recording access to manual files where applicable, e.g. tracking cards, access requests under the Data Protection Act.

Reporting

Once the spot check/audit has been completed a formal report should be produced detailing the outcome. It will include a summary of the findings of the audit, together with observations of non-compliance and recommendations which have been made.

Where non-compliance is observed, this should be recorded as soon as possible, be sufficiently detailed, including all the facts and referring to any relevant evidence. The detail recorded should include an outline of what was observed, where it was observed, who was involved, the date of the observation and why it was considered non-compliant. Each non-compliance observed will be referenced to the section of the relevant CCG Policy or handbook to highlight where there may be an issue with the implementation of a procedure that the CCG has approved, and will have an associated recommendation which should be discussed and agreed with the head of department and other staff as appropriate. Each recommendation will also include a target date for completion and a named individual who will be responsible for ensuring that the recommendation is implemented.

Non-compliance can fall into one of two categories:

Major Non-compliance: this would indicate that the non-compliance has occurred on a regular basis and could potentially have serious consequences.

Minor Non-compliance: these could include one-off occurrences of non-compliance; there are likely to be only minor consequences.

Where a number of minor instances of non-compliance are observed in the same functional area or department, this may indicate a more serious problem within that area. If this is the case, these instances of non-compliance should be combined into a Major non-compliance.

Audit Follow-Up

Reports on audit outcomes including progress on recommendations made will be considered by the group within the CCG that takes responsibility for Information Governance who will monitor progress on actions identified.

Audit Closure

Once corrective action has been checked and agreed as compliant by the auditor, the audit can be formally closed.

PREMISES SECURITY

ID BADGES

All staff should wear their ID badge at all times whilst on the organisations premises or when representing the organisation. ID badges are personal to the user and should not be passed to unauthorised personnel or loaned to other members of staff.

Managers should ensure that any member of staff, whether permanent or temporary, hand in their ID badge on their last day of employment.

The loss of an ID badge should be reported immediately to your line manager and an incident logged.

ACCESS CONTROL

It is essential that access is tightly controlled throughout the organisations premises. Where possible all access to work areas should be restricted.

Visitors should be asked to report to a reception where they will be asked to sign the visitors book recording their name, business, the person they are visiting, time of arrival and departure and then be met by the person who has invited them. Where at all possible, visitors should make appointments in advance and "cold calling" should be strongly discouraged. At the end of the meeting, the visitor will be escorted back to the reception area to sign out, prior to departure.

Members of staff who require access through any door which is controlled via digital door locks or proximity access systems, will be issued with the appropriate code numbers or personal fobs/cards to ensure the security of the area is maintained at the highest level. Code numbers must be kept secure and must never be given to visitors. Such doors should never be latched or wedged open.

Staff should not release any door with controlled access without first checking the identity of the person seeking entry.

Where entry to a working area is by coded access, these codes must be changed on a regular basis or whenever it is felt that the code may have become compromised.

Staff should also be aware of other persons “tailgating”, i.e. attempting to gain access to a controlled access area by closely following them as they enter. If the person is not recognised as a member of staff, or authorised visitor, he/she should be asked to:

- Wait at the door or in a designated waiting area;
- Give details of the person, with whom they have an appointment;
- Await the arrival of an identified member of staff to escort them into the controlled access area;
- At the end of the appointment / meeting the visitor should be escorted out of the controlled access area.

Staff are expected to challenge anyone found in non public areas not displaying a name badge, firstly to ensure that they have a legitimate reason for being there and secondly to remind them of the organisations expectations with regard to use of identity badges.

SMARTCARD SECURITY

Employees are personally responsible for ensuring patient/staff information is protected and only used for specified and lawful purposes. Your Smartcard provides you with the level of access to information you require as part of your role. Smartcards are issued to individual members of staff and must only be used by the person whose name is on the card.

Accessing information using another person's Smartcard is against the law, even if you are authorised to have access to the information. Users of Smartcards must follow the terms and conditions of use – these can be found on the Smartcard application form (RA01).

Care must be taken by everyone issued with a Smartcard to keep it secure and protect their pin against discovery, and cards should be treated with care and protected to prevent any loss or damage.

It is easiest to think of a Smartcard in the same way as you would a credit card and afford it the same protection!

STAFF MUST NOT SHARE SMARTCARDS OR PIN NUMBERS

Smartcard pin numbers must not be divulged, and must only be known to the card holder. Not even RA personnel are allowed to know user pin numbers. Cardholders are not permitted to have more than one card and Smartcards must never be shared or allocated to anyone other than the intended recipient. If staff become aware of an instance where Smartcards/pin numbers have been shared, they must report this immediately to their line manager and an incident must be reported.

Users who have forgotten their pin number should contact the Registration Authority Agent or designated sponsor in order to have their pin number reset.

STAFF MUST NOT LEAVE SMARTCARDS IN COMPUTERS

Smartcards should never be left unattended. Staff must take all reasonable steps to ensure that workstation's are always left secure when not in use by removing Smartcards however briefly the workstation is left unattended. Never leave your Smartcard in the Smartcard reader when you are not actively using it.

STAFF MUST NOT COVER THE PICTURE ON THEIR SMARTCARD WITH THEIR PIN NUMBER

Under no circumstances should pin numbers be written on or attached to Smartcards. Smartcards should not be altered or tampered with in any way.

ANY LOST OR STOLEN CARDS SHOULD BE REPORTED IMMEDIATELY TO YOUR SPONSOR AND REGISTRATION AUTHORITY AGENT SO THEY CAN CANCEL YOUR CARD AND REPLACE IT AS SOON AS POSSIBLE.

Please note that the terms and conditions of smartcard usage is monitored and when an employee signs up to the terms and conditions laid out on the RA01 form, the following condition is agreed to:

By signing the declaration set out in the RA01 Short Form, I, the applicant:

acknowledge that my Smartcard may be revoked or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);

Therefore, any breaches of these terms and conditions will be treated as a disciplinary offence under the organisations disciplinary procedure.

MOBILE MEDIA AND PORTABLE DEVICES

For the purpose of this IG Handbook, a portable device is defined as any device that may synchronise with another computer, for example:

- Laptop and notebook computers
- iPads
- Smart phones, mobile phones and any other mobile system that may fall into this category
- USB memory sticks, (only for temporary storage of information that can in no way be considered confidential, information to be transferred to secure server as soon as practicable and deleted from USB stick)
- MP3/4 players (must not be used at any time for storing person confidential data or commercial information)
- CDs, DVDs
- Any other item that may be utilised to store or transport data.

This list is not to be considered exhaustive.

Any portable device used in connection with the organisation must be encrypted to a minimum of AES-256 bit encryption. There are no exceptions.

CORPORATE MOBILE DEVICES

Asset Management

- All mobile devices issued by the organisation are issued on a one device to one person basis only and must not be shared or used by anyone who is not recorded as the asset owner; this is for audit purposes and to comply with the Data Protection Act 1998.
- Transfer of any device between staff members must only be done via the IT Department.
- Any business related software applications on mobile media devices must be approved and appropriately licenced and recorded on the organisations licence asset register. The IT Department will maintain a software application asset list to ensure licencing conditions are not breached.

SECURITY OF DEVICES

- Any apps downloaded that affect the function of the device will be deleted by IT and not reloaded.
- Do not connect any equipment via the USB port unless it is approved by the organisation.
- Ensure your antivirus is up to date and always activated by connecting regularly to the organisation network.
- You are responsible for the security of the mobile media device at all times whether this is on NHS premises, the premises of other organisations, in the car, on public transport or at home.

If your device is lost or stolen you must report it **immediately** to the IT service desk and the Information Governance team. You must also complete an incident report immediately.

PASSWORDS

- Each device provided by the organisation will require a password to access it. You are not permitted to give that password to anyone else under any circumstances. Each device has a different protocol for passwords.
- You will be required to change your network password regularly and within a maximum of every 40 days ensuring you use a strong password.

- Devices connected to the network such as iPhones and iPads must have a 4 digit PIN enabled to lock the device and screen when not in use.

GUIDANCE AND FREQUENTLY ASKED QUESTIONS

How will I connect to the internet?

The IT Service desk must set this up for you to ensure it is securely connected using a Virtual Private Network (VPN)

How do I set up security for my corporate device?

The IT Servicedesk will set this up for you, please do not alter or attempt to ‘Jailbreak’ your device.

Jailbreaking is the process which removes any limitations placed on the iPad or iPhone's by Apple. Once Jailbroken, users are able to download unlicensed, uncontrolled and pirated applications, extensions and themes that are not otherwise available.

Can I set up an Apple account?

Yes, you will need to do this using your own personal details to be able to download apps at your own expense.

Can I use any Apps for work?

Apps must not be used for storing or transferring any information that belongs to the organisation as they may not be deemed to be secure as per ICO guidelines. This is because some apps hold data in other countries which are not covered by the Data Protection Act or equivalent legislation and therefore security of the data cannot be guaranteed.

For this reason, apps such as Dropbox **MUST NOT** be used.

If a breach were to occur because this data is misused or lost or stolen then we would be held legally responsible as the Data Controller of the data and subject to penalties. This applies to individuals and to the organisation.

Can I download Apps for personal use?

You may download apps for personal use at your own expense.

You need to be aware that use of apps on corporate devices may significantly increase costs to the organisation because data downloads will be increased. Usage will be monitored and re-charges to staff may apply.

How do I access my work emails?

The IT Service desk will provide you with instructions on how to set up your email account using Microsoft Exchange.

Can I access my nhs.net email account on my mobile device?

Yes, you can login using your internet browser and the guidance provided by NHS.net

Can I access websites for personal use?

Yes, but note that if using a corporate device that the organisations guidelines on Email and Internet usage will still apply.

Can I use social media such as Twitter or Facebook for work purposes?

You can use these sites as per the organisations Social Networking guidelines, included in this handbook.

Can I personalise my corporate device?

Yes, but please do not use inappropriate material as a screensaver, background or ringtone which may cause offence.

Can I take my device abroad?

Devices should not be taken outside of the UK because the security cannot be verified once outside the country and therefore data will be at risk.

How can I keep my information safe on my mobile device?

- Do not leave the equipment unattended in a public area.
- Do not allow information to be seen by individuals who do not need to see it.
- Use the minimum information necessary when sending/transferring – removing as much identifying data as possible.
- Do not copy information containing private confidential data or commercial data from the organisations servers/network to an unsecure area or App on your mobile device. If you are unsure please ask the IT Service desk how to store information safely.
- When transporting the equipment in the car it should be stored correctly and out of site i.e. a mobile media device such as a laptop should be placed in its case and stored in the locked boot.
- You must not leave any mobile media device in a vehicle overnight. It must be stored securely in the house or in a locked drawer in a secure office.

What should I do with my mobile device upon leaving the organisation?

- Corporate devices must be handed back to IT via your line manager
- Personal devices must be taken to IT for them to safely remove any corporate data, apps, software etc.

What should I do if I think that my mobile device has been compromised in anyway? e.g. hacked or infected with a virus

Report any incidents or concerns ASAP to the IT Servicedesk for them to investigate and resolve.

MOBILE OR HOME WORKING

The organisation understands that there are occasions when the ability to work away from the office is a necessity. For this reason the following procedures and principles have been developed and must be adhered to at all times:

- No person identifiable or commercially sensitive information should be worked on remotely unless connected securely via the VPN (see bullet points below).
- Users should connect to the network via the organisations virtual private network (VPN). A VPN is a computer network that uses the Internet to provide individual users with secure access to their organisations network. The VPN provides a secure communication between organisation owned hardware (i.e. laptops) connected to non NHS networks and the organisations network. The capability to utilise VPN is automatically included in the build of all the organisations laptops and is comparable to utilising a PC to access information, therefore authorisation to use this facility is not required beyond the initial authorisation for the purchase/use of the laptop.
- It is recommended that all staff use equipment provided by the organisation when working remotely. No equipment, data or software should be removed from the organisations premises without prior line management approval.
- No information should be saved to the hard drive of a laptop, to a USB stick or to any other removable media for the purpose of remote working. This is not an authorised procedure and this practice should cease with immediate effect.
- Emailing work as attachments to either home accounts or work account (if not accessed via VPN) is not an approved method of working remotely either as this leaves ‘footprints’ on the computer.
- Accessing information belonging to the organisation in public accessible areas is discouraged, due to the threats of “overlooking” and theft of equipment. Staff are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

- Computer equipment used away from the organisations sites should never be left unattended when logged in and switched on and must be securely locked away at all times.

- Physical records of individuals (e.g. patients, employees, complainants, those involved with incidents) must only be taken off site if absolutely necessary. This should normally only occur with the agreement of the Line Manager and/or the Caldicott Guardian.

- Records and equipment must always be transported in a secure way e.g. in a sealed container, briefcase, kept in the boot of the car and not visible to the general public. Records must be securely locked as soon as practicable and should not be left in the boot of the car overnight.

- Documents/Records used away from the organisations sites should never be left unattended.

- Records should be returned to the office when no longer needed off-site and in addition, paper records should be logged to reflect that they have been returned and this should be signed and dated by the person returning the records.

- Ensure records cannot and are not seen/viewed by any unauthorised individuals including any other members of the household (including family, friends and neighbours and their children/parents), even if these people are employees of the same organisation.

VIDEO AND TELECONFERENCING

Video and teleconferencing is becoming a powerful way for colleagues to communicate and collaborate, but can be open to abuse both deliberate and accidental as systems are designed to be easy to use with the ensuing security relying more and more on end users than on restrictions built into the software/hardware.

The use of such equipment will also contribute to the organisation’s ability to reduce the need for travel.

As this form of communication is two-way technology, equipment should be located and used where there is the least risk of private activities being accidently seen or overheard.

When arranging the meeting, and sending out invites, this guidance should be included to ensure that all participants are aware of and signed up to the following:

1. All participants must identify themselves at the beginning of the meeting and when speaking, to ensure that the other participants are aware of the speaker.

2. No recording outside of that organised by the Chair shall be made.

3. No participants shall be expected to invite others to take part in the meeting/session without the express consent of the Chair.

4. Headsets should be worn for all meetings/sessions where participants may be overheard by others, and webcams should be used where they cannot be overseen by others outside of the invited participants.

5. Where a participant enters/leaves the session, whilst it is in progress, the Chair must ensure that all participants are aware of the fact, with participants announcing their arrival/leaving with their name and job role etc.

6. At the end of the session the Chair must make sure that all participants are aware that the session has concluded, and if a recording is being made that the recording is stopped at this time.

RESPONSIBILITIES

Chair of Meeting/Session

The Chair is responsible for the overall running of the meeting/session. They must ensure that all participants are introduced at the beginning of the meeting/session, and that they are all able to see and hear each other. The Chair will be responsible for ensuring that reasonable adjustments are put in place where a participant has an access need.

They will be responsible for the facility itself for the duration of the meeting/session, from ensuring all is in order before the meeting, co-ordinating with IT Technical Staff if required, and ensuring all is in order at the end of the meeting. They are also required to ensure that all participants have signed a “Compliance” statement form before the meeting/session begins.

All participants invited to the meeting/session should be aware as to whether the meeting/session is being recorded or not. They should also ensure that no additional recordings are made by participants themselves.

If the session is recorded, the Chair is responsible for ensuring that all participants have given their consent and that there is a verbatim copy available for all participants if requested.

Meeting/Session Participants

All participants are expected to adhere to this guidance, and return the signed “Compliance” forms that they are given, either at a training session or before their first video or teleconferencing meeting/session.

No additional recordings are to be made without the express permission of the Chair before the meeting/session commences.

They must wear headsets to ensure that other staff may not overhear the conversations, and any webcams used should not be overseen by others where possible.

Training & Implementation

Training on the use of the software/equipment will be provided. Contact can be made via the local IT Servicedesk.

All users will need to familiarise themselves with this guidance before access to the systems.

RECORDS MANAGEMENT

Records are a valuable resource because of the information they contain, however, the information is only useable if it is correctly recorded in the first place, is regularly updated and is easily accessible when it is required.

Information Lifecycle Management ensures that as an organisation we manage information through every phase of its existence – from creation right the way through to destruction.

Identification

All records should be clearly identifiable from the file cover, which should include an accurate title or description of the information contained and where appropriate the department or service to which it relates.

Classification

Both electronic and paper records and documentation may require classification. Records can be classified into several categories, such as draft, confidential, commercial in confidence. If a confidential or commercial in confidence mark is required, consideration must be made in relation to the retention, storage and dissemination of this information. Staff must also be aware that records classified as confidential and commercial in confidence within the organisation may also on occasion be accessible to the public under legislation such as the Freedom of Information Act 2000.

Version Control

For all records created, version control is important as documents undergo revision and updating on a regular basis. Version control should be used to manage revisions of a document, enabling the reader to differentiate one version of a document from another. It is particularly important as version control should also be used to clearly identify a final version of a document, which will then assist with referencing and, when required, off-site storage.

Most documentation will require the use of simple version control techniques such as the use of naming conventions, version numbering to distinguish one version from another; it is recommended that this practice is used for all documentation where more than one version exists. Use of numbering within version control should be used to reflect major changes from minor (i.e. whilst in development, version control should be version 0.1, each amendment to the document after should increase the last digit by 1. Once approved version 1.0, any amendments should repeat the process in the same way as previously stated, if further approval is required version 2.0 and so on). The version number and date should be clearly visible within the document, such as the front cover with the version number being contained within the footer of the document to ensure that it is visible on every page.

Retention

All records that are created have an associated retention period. The length of the retention period depends on the type of record and its importance to the business of the organisation and the legal requirements.

All documents and records should be reviewed on an annual basis to ensure that appropriate storage and retention is maintained.

To ensure that all records are retained for the minimum recommended retention period the Records Management NHS Code of Practice Part 2 should be reviewed to ensure that the minimum retention period is achieved: – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf

NHS England have also published guidance more aimed at Commissioning Organisations that can be used in conjunction with the DoH guidelines. A copy of NHS Englands **Corporate Records Retention – Disposal Schedule and Guidance** can be found at http://www.england.nhs.uk/ourwork/tsd/ig/ig-resources/and scrolling down to Records Management.

DIGITAL RECORDING OF MEETINGS AS AIDE MEMOIR TO MINUTE TAKER

The digital recording of meetings as an aide memoir to the minute taker is often required. If the meeting is to be recorded for this purpose please follow the guidance below:

- There would need to be agreement by the members to audio record the meeting, explaining that this recording would be used purely as an aide memoir for the minute taker to ensure an accurate transcript of the meeting.
- Written consent should be obtained by the members agreeing for the meeting to be recorded.
- New Terms of Reference would be required identifying agreement to record the meeting, the reason for recording the meeting, where/who will have the only copy of the audio recording and when the recording will be destroyed.
- The Chair of the meeting has discretion to stop or suspend recording if, in their opinion, continuing to do so would prejudice proceedings at the meeting.

- Prior to the meeting, communications should be sent notifying members the meeting will be digitally recorded, this should also be identified on the formal agenda.
- All panel members should be advised that the digital recording will be held for
  - Same retention as the written transcription for high / board level meetings
  - 3 months for lower level meetings

  after the written transcript has been ratified by all members and then destroyed. A flag would need to be set to ensure the recording is deleted after this time.
- As the audio recording would be a record for the above agreed time, it is important to record the destruction of this record to assist in audit purposes.

RETENTION OF NOTES AND RECORDINGS TAKEN AS AIDE MEMOIR FOR A MINUTE TAKER

For High Level / Board Level meetings; notes and recordings should be retained for the same length of time as the written transcription

For other lower level meetings; it is acceptable to destroy notes and recordings after 3 months.

ELECTRONIC RECORDS

Electronic documents that contain information that supports a decision making process of any description, undertaken by any directorate/department or service must be managed to the same standards expected of paper records and for this reason, they must be retained on a corporate shared drive or appropriate intranet site.

Access

Access to the shared drive should be managed to ensure that access to the information contained electronically is controlled in the same way as paper documents. This should be done by restricting folders to staff groups and not by password protecting individual documents as this may make them inaccessible in the future should you forget the password. Even the IT Service will be unable to remove passwords from Microsoft documents.

Having a logical filing structure will enable the quick and efficient filing and retrieval of records when required and enhance lifecycle management arrangements i.e. archiving, migration to another format or destruction.

Tracking should also take place to ensure that the cross-referencing of electronic records with their paper counterparts can take place and be relied upon that version control is maintained both electronically and in paper format.

The organisation should use a clear and logical filing structure for electronic records to support the retrieval and retention of the records. Ideally, the filing structure should reflect the way in which paper records are stored to ensure consistency. However, where it is not possible to do this names allocated to files and folders should be done in a way that allows intuitive filing.

Electronic Record Naming

File Names' are the names that are listed in the computers file directory and that are allocated to new files as they are saved for the first time. By naming records consistently, this will enable staff to distinguish similar records at a glance.

Naming records according to an agreed convention will make naming easier for staff as a "re-think" process will not be required on every occasion.

Recommendations to follow:

- Keep file names short but meaningful;
- Avoid unnecessary repetition and redundancy in file names and file paths;
- Use capital letters only when naming top level folders;
- When including a number in a file name always give it as a two digit number, i.e. 01-99 (unless it is a year or a number with more than two digits);
- Staff names should **not** be used as file names (i.e. BOB SMITH or BOBS FOLDER);
- Avoid using common words such as 'drafts' or 'letters' at the start of file names unless it will assist with record retrieval;
- Order the elements in the file name in the most appropriate way to retrieve the record;
- A file name should not be replicated to subfolders within the file (i.e. Audits 2010 and Audits 2011 within the Audit Folder);
- Dates should always follow the recommended format, YYYY-MM-DD, to ensure documents are stored in chronological order.
- Avoid using common words such as Draft, Letter or memo at the start of a file title.
- Make sure elements in the file title are ordered in the most appropriate way to retrieve the record.

- Correspondence record titles should always include the following elements: name of correspondent, subject description (if not already in folder name), date of letter, email etc. and ‘rcvd’ if incoming correspondence.
- Apply version number or status to documents where required.
- Avoid use of non-alphanumeric characters in file names (i.e. * : / \ < > “ ! + = £ $ &,).

STORAGE OF ELECTRONIC RECORDS

The shared drive is to be used by all employees as a central location to store all electronic documents.

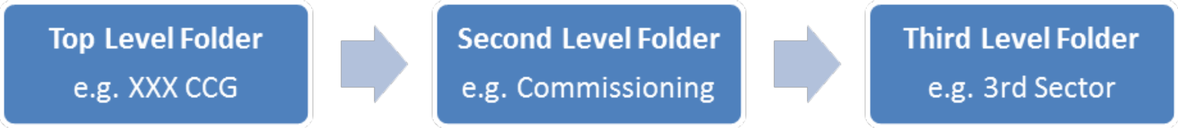
All work related files (documents, spreadsheets, etc.) must be stored on the shared network and data that is for your personal use only is stored on your personal drive (you may know this as “My Documents”, U Drive or I Drive).

The disk capacity for the storage of files is limited. It is not permitted to save music files or digital images from personal cameras to the network. The IT Service reserves the right to delete such files without notice.

Access to folders should be restricted, based upon the users employment position and requirement under that post to access information.

CREATING FOLDERS IN THE SHARED DRIVE

If a restricted folder needs to be created in the shared drive, please contact the IT service stating the name of the folder to be created, where it is to be located (please note that restricted folders can only be created on the top 2 levels of the n drive as per example below), and the names of the people who are to be granted access to the restricted folder.



Top Level Folder
e.g. XXX CCG

Second Level Folder
e.g. Commissioning

Third Level Folder
e.g. 3rd Sector

If a folder or file on the shared drive needs to be moved, this must be done by copying and pasting. Once you can see the file in the new location, go back to the original location and delete. Do not “Drag and Drop”. If the file/folder is dragged, it will retain the access permissions associated with its original location. This can cause the folder/file to become inaccessible to staff in the future.

PAPER RECORDS

Good quality documentation standards are essential to provide accurate records of the organisations activities.

Filing

Records and documentation contained within a paper file or filing system should be securely fastened using treasury tags and folder ties appropriate to the record type. Loose papers and plastic wallets should be securely fastened as loose documentation even if placed in a plastic wallet can be easily lost, misplaced or damaged. The use of sellotape and staples to secure paper and documents into files is not recommended (staples can be used to staple a document together; however, this method is not to be used as a secure file fastening).

Record Naming

It is expected that the organisation follows the advice and recommendations issued by The National Archives, i.e.:

- Give a unique name to each record;
- Give a meaningful name which closely reflects the record contents;
- Express elements of the name in a structured and predictable order;
- Locate the most specific information at the beginning of the documentation name and the most general information at the end
- Give a similarly structured and worded name to records which are or can be linked (e.g. an earlier or later version)

Indexing

An index (or register) should be used primarily to signpost staff to the location that paper records are retained (i.e. the relevant folder or file within a filing cabinet), however, it can also be used by staff to identify the information contained within those records. An index should be developed to be a user-friendly structure to aide staff in the easy location and retrieval of records and documentation (It is not recommended that staff file or retain records in desk drawers as this limits accessibility and may lead to issues with version control as well as record naming and indexing or continuity of patient care). It is requested that all records are retained in central filing systems ensuring accessibility to all appropriate staff as required.

Tracking and Tracing

Records are created and captured in order to be used; therefore record keeping systems must include effective mechanisms for tracking and tracing their whereabouts and use. Effective procedures must be in place to ensure swift retrieval, an audit trail of use and for their accurate return.

A comprehensive tracking system should include:

- Effective aides to identify documents and records and provide the location details and highlight any restrictions appropriate to it.
- The use of tracer cards and a register to track records that have been accessed and relocated.

Depending on the nature of the document/record, authorisation for access may be required. Where most records are available to the public an authorisation procedure is not necessary. However, where records are sensitive due to data protection, commercial confidentiality or security issues, these documents and records will need to be tracked and monitored to ensure that appropriate authorisation processes are in place to approve staff access.

Effective tracking will ensure that records can always be located when required and that records remain controlled and secure, thus enhancing their reliability and authenticity.

As a minimum, a tracking system should include:

- The record Reference or unique identifier
- Title or description of the record
- The individual (including job title, telephone number and e-mail address),department and location accessing the record
- Date and signature confirming removal and return of record

Tracking systems ensure records are appropriately tracked when records are sent between staff/departments. However, if a record is being permanently transferred the Record Review and Disposal List should also be completed. Please contact the IG team for this document.

Record Maintenance and Storage

Records should be retained in facilities appropriate to the record type (i.e. confidential information should not be retained on open shelves in open office areas), environmental considerations such as excessive lighting, damp or flooding must also be considered when decisions are made for the housing of records in the work area. Record storage facilities should not be overcrowded and should allow for easy retrieval and return of records.

The papers and documentation contained within records should be arranged and retained in a logical manner, which has structure and is ordered by chronology.

Duplicate documentation should be removed where possible. When a file becomes too large or excessive a second volume should be created and indexing and version control used.

Directorates, Departments and Service Areas should record all record types on the Information Asset Register, this in turn will be used by the organisation as a file plan, in turn will be used for the auditing of records.

Information contained within records may be required to meet the requirements of legislation such as the Freedom of Information Act (2000) and as such these records must be accessible to ensure that specific time limits set out within the act are adhered to. Clinical records may be required to meet the requirements of legislation such as the Access to Health Records Act (1990) and Data Protection Act (1998).

Records should be stored securely and not left unattended or accessible to staff who are not authorised to access them. Where records are removed from the work area a tracking system should be used.

FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOI) came into force on 01st January 2005. http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1 The Act is designed to promote openness and transparency within public authorities.

Who can make a Request?

- Anyone can make a freedom of information request – they do not have to be UK citizens, or resident in the UK.
- Freedom of information requests can also be made by organisations, for example a newspaper, a campaign group, or a company.
- Employees of a public authority can make requests to their own employer, although good internal communications and staff relations will normally avoid the need for this.

What information is covered by the Act?

- The Act covers all recorded information held by a public authority. It is not limited to official documents and it covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings. Nor is it limited to information you create, so it also covers, for example, letters you receive from members of the public, although there may be a good reason not to release them.

- Requests are sometimes made for less obvious sources of recorded information, such as the author and date of drafting, found in the properties of a document (sometimes called meta-data). This information is recorded so is covered by the Act and you must consider it for release in the normal way.

- If a member of the public asks for information, you only have to provide information you already have in recorded form. You do not have to create new information or find the answer to a question from staff who may happen to know it (i.e. it's in their head)

- The Act covers information that is held on behalf of a public authority even if it is not held on the authority's premises. For example, you may keep certain records in off-site storage, or you may send out certain types of work to be processed by a contractor.

- Where you subcontract public services to a private company, that company may then hold information on your behalf, depending on the type of information and your contract with them. Some of the information held by the external company may be covered by the Act if you receive a freedom of information request.

What are the organisations obligations under the Act?

As an organisation, there are two main obligations under the Act. You must:

- publish certain information proactively.

- respond to requests for information where the information is not proactively published.

Making information available is only valuable to the public if they know they can access it, and what is available. You should:

- publicise your commitment to proactive publication and the details of what is available.

- publicise the fact that people can make freedom of information requests to you;

- provide contact details for making a request, including a named contact and phone number for any enquiries about the Act; and

- You should communicate with the public in a range of ways. This is likely to include websites, noticeboards, leaflets, or posters in places where people access your services.

Recognising an FOI Request

Where any of the following points below apply, the request should be treated as an FOI Request:

- Have you received the request in writing? (either email/fax/handwritten)

- Have they provided a contact name?

- Is the request for information that is not readily available in a published document that the organisation produces? (for example; Public leaflet, brochure of services etc.)

- Is the request for information that you do not have available to you in your day to day duties?

Processing an FOI Request

- All requests should be forwarded to: http://www.dudleyccg.nhs.uk/freedom-of-information/

- The organisation has only 20 working days to respond to requests
- The clock starts the next working day after you receive the request
- If the request is not clear enough and requires further clarity the organisation can go back to the applicant
- On contacting the applicant for further clarification the clock stops until they reply.
- On receipt of the clarification you should re-commence the clock from the point at which it stopped (do not restart!).

Remember: As there is a statutory timeframe for the organisation to respond to FOI requests, it is therefore imperative that requests are dealt with quickly and treated as high priority items

SUBJECT ACCESS REQUESTS

Patients and employees have a right under the Data Protection Act 1998 to access personal data about themselves which is held in either electronic or manual form by the organisation. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 (except for records relating to deceased patients). This type of request is known as a Subject Access Request.

All Subject Access Requests must be made in writing. Within all applications for access to records the applicant will need to prove their identity.

As per the Department of Health's "Guidance for Access To Health Records Requests" (http://systems.hscic.gov.uk/infogov/links/dhaccessrecs.pdf):

> ***"Although the DPA states 40 days to comply, a Government commitment requires that for health records requests should normally be handled within 21 days."***

The administration of requests for access to records (subject access requests) will be undertaken by a trained Subject Access administrator. Clinically trained leads will review records prior to release under the Data Protection and Access to Records Acts. The CSU Information Governance team are responsible for training Subject Access administrators and will provide advice and guidance on all aspects of Data Protection and Access to Records Acts. Additional guidance can also be provided by the Caldicott Guardian.

All Subject Access Requests will be dealt with following standard operating procedures set out by the CSU Information Governance Team, ensuring that NHS England are made aware of all requests received and the outcome/completion of each request.

If you receive a request for access to records, or any queries regarding access to records, the request/query should be **immediately** forwarded to the Subject Access administrator who will ensure that the request is processed and responded to within the time frame specified by the relevant Act.

INFORMATION GOVERNANCE INCIDENTS

All employees have a responsibility to raise events and incidents that they identify.

All staff have a responsibility to raise anything they believe may be an incident, even if it transpires to be a near miss, rather than not raise it at all. What may at first appear to be of minor importance may, on further investigation, be found to be serious and vice versa.

What is an Information Governance related Serious Incident Requiring Investigation (IG SIRI)?

As a guide, any incident involving the actual or potential loss of personal information that could lead to identity fraud or cause other significant impact to individuals should be considered as serious. This includes any incident which involves actual or potential failure to meet the requirements of the Data Protection Act 1998 and/or the Common Law Duty of Confidentiality would be considered an IG SIRI. It does not matter what type of media is involved, so includes information held electronically and paper records.

Examples of IG SIRIs include:

- Unlawful access, disclosure or misuse of confidential data, whether deliberate or in error, even if the information itself hasn't actually been accessed.
- The loss of data in any format, whether whilst in transit from one business area to another location or not.
- Recording or sharing of inaccurate data
- Information security breaches and inappropriate invasion of people's privacy
- Failure to dispose of information (electronic and paper) containing personal data to an appropriate technical and organisational standard.
- Technical security failing (including hacking)
- Corruption or inability to recover electronic data

What isn't an IG SIRI?

Loss or theft of **encrypted** removable media (laptops, CDs, USB memory sticks, media cards, PDAs) is not a IG SIRI unless you have reason to believe that the protection applied to the device has been breached and personal data accessed inappropriately. However, the loss of such media should still be reported as a "near miss" in terms of IG. Another example of a "near miss" would be the loss of a smartcard (no actual data loss, just the potential for unauthorised access to data).

If the CCG receives data in error, for example a fax or email is sent to the CCG which was intended to go to another organisation, unless there is a requirement in the CCGs contract with the sender organisation, then the CCG is not responsible for reporting the incident. Instead, the CCG must ensure that the sender is informed of the error and request that the incident is reported through the sender organisations incident recording procedures. If the information is received by fax, a template form which can be used to advise the sender is included in Appendix G of this handbook. The CCG should provide assurance to the sender that the information has been disposed of securely, unless the sender requests that the information is returned, for example if it is an original record that has been received.

How should IG SIRIs be reported?

Dudley CCG' Process and Policies for IG Incident Reporting is subject to review.

IG SIRIs should be reported in the same way as any other incident.

In the first instance report the incident to your line manager who will notify the CCGs IG Support Officer, who will support you in reporting the incident via the CCGs Incident reporting tool. It is vital that any incidents or near misses, even if they have not yet been confirmed, are reported as soon as practically possible (and no later than 24 hours of the incident occurring or being identified during the working week). The CCG is required to report any incidents with a severity level of 2 (please see below for explanation) within 24 hours of their occurrence so it is imperative that any potential incidents are reported and their severity level assessed within this timescale.

Early information, no matter how brief, is better than full information that is too late. If there is any doubt as to whether or not an incident has occurred, the Information Governance team should be contacted for advice.

What is the Information Governance Incident Reporting Tool?

Alongside the CCGs local incident reporting procedures, there is also a national IG incident reporting tool included within the IG toolkit.

The Information Governance Incident Reporting Tool is an online tool hosted on the secure Information Governance Toolkit website.

- It is the Department of Health (DH) and Information Commissioner's Office agreed solution for reporting personal data security breaches.
- From June 2013 all Organisations processing health and adult social care personal data are required to use the IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the DH, ICO and other regulators.
- **If the outcome of the severity is Level 2 (reportable) an email notification will be generated by the system and sent to the HSCIC External IG Delivery Team, DH, ICO and escalated to regulators, as appropriate**.
- Organisations can only see incidents recorded against their organisation code. They cannot view other incidents until information is published on the Information Governance Toolkit website.

Dudley CCG have decided that…

Only level 2 incidents to be recorded on the toolkit

The CCGs IG Support Officer (IGSO) has access to the Information Governance Incident Reporting Tool and will be responsible for recording incidents on the tool, although access can be granted to other members of staff as required by the CCG.

Assessing the severity of an IG SIRI

When notified of an IG SIRI, the IGSO will undertake an assessment by using the Health and Social Care Information Centre checklist guidance to determine the severity of the incident. The CSU Information Security Officer will verify the IGSOs assessment.

There are three severity levels at which an IG Incident can be assessed:

0. Near miss/non-event
1. Confirmed IG SIRI but no need to report to ICO, DH and other central bodies.
2. Confirmed IG SIRI that must be reported to ICO, DH and other central bodies.

To allow the severity of the incident to be assessed, along with details of what has happened, why and how, the following information **must** be provided as part of the incident report:

1. No. of individuals to whom the data relates
2. Description of the content of the data – what identifiers were included, was there any clinical information and if so, what level of detail, are there any sensitivity factors such as mental health info, safeguarding info.
3. Format of the data (paper, electronic), if electronic was the data encrypted or password protected

When the severity level has been determined, the local incident report must be updated to include the severity level and the incident will be reported on the IG toolkit.

The IG Support Officer will keep a record of all incident severity assessments, a summary of which will be reported to the CCGs IG group and in the quarterly SIRO report, along with any outcomes of the incidents/near misses.

If an incident is assessed as a level 2, the CCGs IG Lead, SIRO, Caldicott Guardian and Accountable Officer must be notified immediately, and the incident must be recorded on the IG toolkit within 24 hours of the incidents occurrence.

IG SIRI Investigations – Level 0 and Level 1

In the case of level 0 or level 1 IG SIRIs, the IGSO, with the support of the CSU Information Security Officer will undertake a brief investigation to determine:

- What happened?
- How and why did it happen?
- What can be done to avoid/reduce the likelihood of this happening again?

The outcomes of this investigation will need to be included within the details of the record created for the incident in the CCGs incident reporting tool. They will also be notified to the CCGs IG Lead, SIRO and Caldicott Guardian as appropriate depending upon the nature of the incident.

IG SIRI Investigations – Level 2

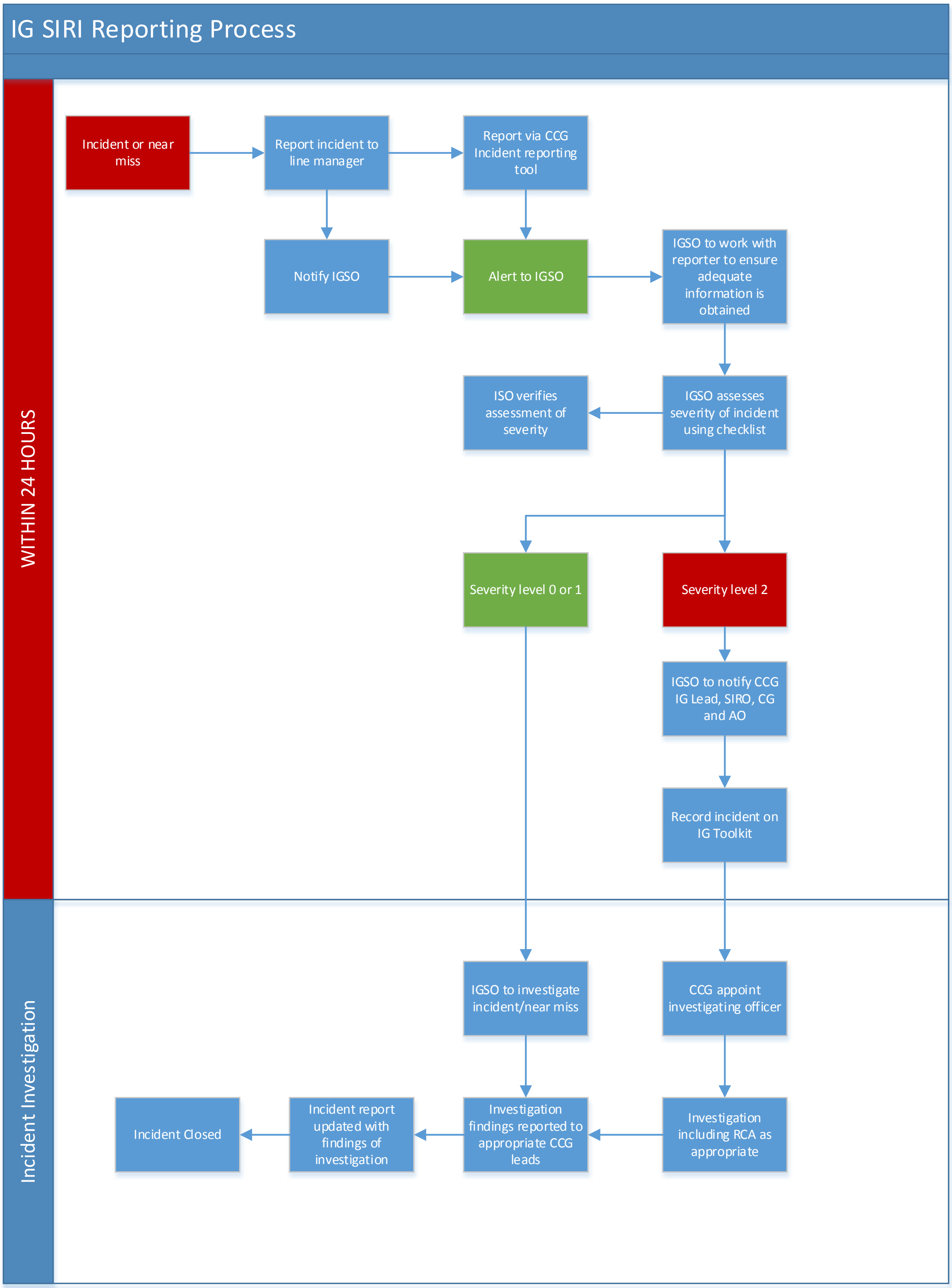
Level 2 SIRIs (those which must be reported on the IG toolkit and are notifiable to the ICO and DH), must be subject to a Root Cause Analysis Investigation. This will be undertaken by an investigating officer who will be appointed by the CCG and will be supported by the IGSO and Information Security Officer. Tools to aid this process can be found at http://www.nrls.npsa.nhs.uk/resources/?entryid45=59847

Informing Data Subjects

Consideration should always be given to informing data subjects when personal confidential data about them has been lost or inappropriately placed in the public domain. Where there is any risk of identity theft it is strongly recommended that this is done. This decision should always be made by the CCG in consultation with their Caldicott Guardian and the Information Security Officer, taking into account the balance between transparency and potential distress/harm that may be caused to the data subjects.

IG SIRI Reporting Process

PROCESS WITH ONLY LEVEL 2 SIRIs REPORTED ON IGT


IG SIRI Reporting Process
WITHIN 24 HOURS
Incident or near miss
Report incident to line manager
Report via CCG Incident reporting tool
Notify IGSO
Alert to IGSO
IGSO to work with reporter to ensure adequate information is obtained
ISO verifies assessment of severity
IGSO assesses severity of incident using checklist
Severity level 0 or 1
Severity level 2
IGSO to notify CCG IG Lead, SIRO, CG and AO
Record incident on IG Toolkit
Incident Investigation
IGSO to investigate incident/near miss
CCG appoint investigating officer
Incident Closed
Incident report updated with findings of investigation
Investigation findings reported to appropriate CCG leads
Investigation including RCA as appropriate

APPENDIX A - INFORMATION GOVERNANCE INDUCTION CHECKLIST – LINE MANAGER

To be completed by Line Manager on first day of employment.

Name of New Employee:	
Job Title:	**Date Started:**
Induction provided by **Name:**	**Job Title:**
Date of Induction:	

Network and Shared Drive Access	**Date**
Network access has been requested from the IT Service desk	
Required access permissions (e.g. for shared drive) have been identified and requested	

Key Documents		
I confirm that I have received a copy of, read and understood the following:		
	Date	**Signature**
Information Governance Policy		
Information Governance Handbook		

Training

	Date
NHS IGTT Induction Module(s) completed successfully	
Additional Information Governance training for job role has been identified:	Please tick as appropriate
Information Risk	
Privacy Impact Assessments	
Caldicott and Data Protection	
Corporate Records Management	

Information Governance Team Contact Information

informationgovernance@staffordshirecss.nhs.uk
/ information.governance@lancashirecsu.nhs.uk

01254 282999 / 01782 298249

APPENDIX B - INFORMATION GOVERNANCE INDUCTION CHECKLIST – INFORMATION GOVERNANCE SUPPORT OFFICER

Name of New Employee: (please print)			
Start date:		**Job Title:**	
Temp / Perm		**Site:**	
Name and Job Title of Manager: (please print)			

This checklist is to be completed by the Information Governance Support Officer and the new employee **within two weeks of the start date**.

Introduction to information Governance	**Complete**	**Date**
What is Information Governance?		
How does IG affect staff, patients and the organisation?		
Who is responsible for Information Governance? • *Senior Information Risk Owner* • *Caldicott Guardian* • *IG Lead* • *All Staff*		
Staff Handbook • Where is it kept? • Signed?		
What is Personal Confidential Data? • Definition		
IG Working Practice	**Complete**	**Date**
Password Security • Do not Share • Keep Secure • Password Format Best Practice		
Always lock your PC • How to do it?		

Screen Position - Ensure no-one can overlook your screen		
Security of Information - Ensuring information is routinely locked away - Home/Remote Working - Transporting Information - Mobile Media		
Incident Reporting - What is an IG Incident? - What is the process for recording?		
Security ID Badges		
Security of Smart Cards		
Preparing to leave my desk - Clear Desk Policy - Locking Away Equipment		
What is a safe Haven?		
IG Support	**Complete**	**Date**
Key Staff within CSU - IG Manager - Information Security Lead - Designated IG Support Officer		
Contact Details		
Training	**Complete**	**Date**
How to log onto the E-Learning to complete Introduction to Information Governance		

I confirm that I have read, listened and understood all aspects that were discussed as part of my IG induction. I have been given sufficient opportunity to ask questions where processes may have not been clear and I know who to contact should I have any additional IG related questions.			
To be completed by the New Employee:			
Signed:		**Date Signed:**	
To be completed by the line Manager:			
Line Manager Confirmation:		**Print Name:**	

APPENDIX C - INFORMATION SECURITY - REQUEST FOR EMAIL ACCESS FORM

Name of requestor:	
Job title:	
Date of request:	
Name of staff member:	
Email address of staff member:	
Impact assessment	
Purpose of Access: Please outline the reasons for requiring access to emails	
Please list any potential adverse impacts: i.e. are any likely adverse impact of the monitoring arrangement, such as intrusion into the private lives of staff and others, or interference with their private e-mails (bearing in mind that the private lives of staff can, and usually will, extend into the workplace), impact on the relationship of mutual trust and confidence that should exist between workers and their employer?	

Will the staff member be notified that their emails have been accessed?
□ Yes □ No, please specify why:
How long is access required for? Please specify duration or “ongoing”

Approval	
Line Manager/Senior Manager	
Name:	
Job Title:	
Date:	
Information Governance	
Name:	
Job Title:	
Date:	

Appendix D - Information Sharing Agreement Checklist

Document Title	
Document Owner	
Job Title	
Email	
Date submitted	
IG Support Officer	

	Please tick:		**Document Reference**	**Comments**
	Yes	**No**		
Has the purpose of the sharing (aims and objectives) been described? Why is the sharing necessary?	□	□		
Is there an explanation of how the agreement sits with other information sharing agreements in operation, e.g. is this a tier 2 agreement, if so which tier 0 and tier 1 does it sit under?	□	□		

	Please tick:		Document Reference	Comments
	Yes	No		
Who are the parties to the information sharing? Are there any parties to the agreement who are not partners to the sharing, e.g. CCG as commissioner.	☐	☐		
Who is the Data Controller for the shared data? Will any of the partners be Data Processors? (Please see ICO Guidance: Data Controllers and Data Processors for guidance)	☐	☐		
Specify the nature of the data each agency will share – is the specific data set to be shared defined?	☐	☐		
Has the requirement to use identifiable/pseudonymised data been explained and justified?	☐	☐		
Has a legal basis been identified for the sharing? Is the legal basis correct/applicable?	☐	☐		
If consent is the legal basis, does the agreement explain: • How consent will be obtained; • Establishing fitness to give consent; • Recording consent; • Time limits for consent;	☐	☐		

	Please tick:		Document Reference	Comments
	Yes	No		
• What if consent is withheld.				
Has a PIA been conducted? Are the results described in the agreement? Is the PIA included as an Appendix?	□	□		
Fair Processing – how will data subjects be informed of the data sharing?	□	□		
Has a post holder within each sharing partner been identified as responsible on a day-to-day basis for this data exchange?	□	□		
Has a post holder within each sharing partner been identified as responsible for ensuring the accuracy of any data exchanged?	□	□		
Are procedures included for checking data quality before sharing?	□	□		
Does the agreement explain how any problems, for example with data accuracy, will be rectified by all parties to the sharing?	□	□		
How will a record be kept of what information has been shared and when?	□	□		

	Please tick:		Document Reference	Comments
	Yes	No		
What is the process for transfer/exchange of data?	☐	☐		
What security measures are there for the transfer/exchange of data?	☐	☐		
Who in the receiving agencies will have access to the data and what purposes can the data be used for? Process for starters/leavers in these posts? Confidentiality clauses? Training?	☐	☐		
Are the security measures to be implemented to ensure stored data is protected outlined in detail? (Both electronic and physical storage, technical and organisational security.)	☐	☐		
Is a procedure to be followed if there is a security breach/breach of confidentiality? Responsibilities for incident reporting /notifying sharing partners?	☐	☐		
Are there any special contingency requirements in case of interruption to the data sharing arrangements?	☐	☐		
Is a retention period for the shared data defined?	☐	☐		
Is there a procedure for what happens when the data reaches its retention period? Are disposal procedures	☐	☐		

	Please tick:		Document Reference	Comments
	Yes	No		
included? What happens if sharing stops before this time/if agreement is terminated for any reason?				
Does the agreement permit any further use of the shared data? What is the process to be followed if a partner wishes to use the data for purposes other than defined in the agreement?	□	□		
Does the agreement include a complaints procedure place to address complaints relating to inappropriate disclosure or failure to disclose personal information?	□	□		
How will the sharing partners deal with requests for access to shared information, i.e. subject access requests? Is there a Common approach to subject access (especially when an access request is to personal data originating from another party to the agreement)?	□	□		
How will the sharing partners deal with requests for access to information about the sharing, i.e. Freedom of Information requests?	□	□		
Does the agreement include any indemnity? What procedures are there should there be enforcement action undertaken by the Information Commissioner (or any other regulator that has remit with respect to the	□	□		

	Please tick:		Document Reference	Comments
	Yes	No		
processing of personal data)				
Is a review schedule for the agreement included? Does the agreement explain the process for redrafting or refining the text of the agreement?	□	□		
Does the agreement describe the implication/process for one of the sharing partners withdrawing from the agreement? Does it include how additional sharing partners can be added to the agreement?	□	□		
Is closure/termination of the agreement addressed? Both natural end of agreement and premature termination.	□	□		
Have appropriate signatories been identified for each sharing partner?	□	□		

	Please tick:		Date	Comments
	Yes	No		

	Please tick:		Date	Comments
	Yes	No		
Agreement approved to go for signature? ***(Please delete additional rows if approved on first review)***	□	□		
Agreement approved to go for signature?	□	□		
Agreement approved to go for signature?	□	□		
Agreement approved to go for signature?	□	□		
Agreement approved to go for signature?	□	□		
Agreement approved to go for signature?	□	□		

APPENDIX E - PRIVACY IMPACT ASSESSMENT - CHECKLIST

Key Information – please be as comprehensive as possible.	
Project Name:	
Description of project:	*Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.* *You may find it helpful to link to other relevant documents related to the project, for example a project proposal*

Will the project involve any data from which individuals could be identified (including pseudonymised data)? **(Yes/No)**	

IF NO THEN YOU DO NOT NEED TO ANSWER ANY FURTHER QUESTIONS AND A PIA IS NOT REQUIRED.

Key Contacts	
Project Manager Name & Job Title:	
Project Manager Email:	
Project Manager Phone:	

Key Stakeholder Names & Roles:	

Screening Questions	YES or NO
Will the project involve the collection of **new** information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services	
Is the information to be used about individuals' health and/or social wellbeing?	
Will the project require you to contact individuals in ways which they may find intrusive?	

If any of the screening questions have been answered "YES", then please continue with the Privacy Impact Assessment Questionnaire (below).

If all questions are "NO", please return the document to the Information Governance Team and **do not** complete a Privacy Impact Assessment. Please email the completed screening to Helen.dewaine@nhs.net

APPENDIX F - PRIVACY IMPACT ASSESSMENT – QUESTIONNAIRE

Use of personal information	
Description of data:	*e.g. name, address, date of birth, NHS number, gender, clinical or other health information, ethnicity.*
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	
Will the information be new information as opposed to using existing information in different ways?	
What is the legal basis for the processing of identifiable data? **If consent, when and how will this be obtained and recorded?**	*e.g. explicit data subject consent, s251 support, statutory power.*
Who will be able to access identifiable data?	*This should include details of any data processors / contractors and sub-contractors and any proposed overseas transfers*.

Will the data be linked with any other data collections?	*Please specify and provide business reason / information requirement*
How will this linkage be achieved?	*Who will undertake the linkage and using what identifiers?*
Is there a legal basis for these linkages?	*i.e. is it within the terms of any prior consent? Is it within the scope of any statutory justification?*
What security measures will be used to transfer the data?	
What confidentiality and security measures will be used to store the data?	*i.e. contractual arrangements with data processors, contractual arrangements with their staff as well as physical and technical security measures*

How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	*e.g. Data retention, redaction and disposal policy. Include arrangements if the project is withdrawn/ stopped*.
What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?	*e.g. oversight body / committee, security audit and risk review procedures.* *This should also include contingency planning against accidental loss, destruction or damage to personal data.*
If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA? **Is there functionality to respect objections/ withdrawals of consent?**	*This should include how personal data is located and procedures for explaining the information in the record e.g. coded data, to the individual.* *How third party and seriously harmful information will be handled and how grounds for withholding information will be managed.*
Are there any plans to allow the information to be used elsewhere either in the CCG, wider NHS or by a third party?	

Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.

Does any data flow in identifiable form? If so, from where, and to	

where?	
Media used for data flow? **(e.g. email, fax, post, courier, other – please specify all that will be used)**	

Consultation requirements

Part of any project is consultation with stakeholders and other parties. In addition to those indicated "Key information, above", please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information.

It is the project's responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations.

Privacy Risks

List any identified risks to privacy and personal information of which the project is currently aware. Risks should also be included on the project risk register.

Risk Description (to individuals, to the CCG or to wider compliance)	Proposed Risk solution (Mitigation)	Is the risk reduced, transferred, or accepted? Please specify.	Further detail if required

Further information

Please provide any further information that will help in determining privacy impact.

Following acceptance of this PIA by Information Governance, a determination will be made regarding the privacy impact and how the impact will be handled. This will fall into three categories:

1. **No action is required by IG excepting the logging of the Screening Questions for recording purposes.**
2. **The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.**
3. **The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.**

It is the intention that IG will advise and guide those projects that require it but at all time will endeavour to ensure that the project moves forward and that IG is not a barrier unless significant risks come to light which cannot be addressed as part of the project development.

Please email entire completed document to Helen.dewaine@nhs.net

APPENDIX G- FAX RECEIVED IN ERROR NOTIFICATION

NHS
Dudley
Clinical Commissioning Group

To: [to] Fax No: [fax no]

From: [from] Date: [date]

*****FAX RECEIVED IN ERROR*****

This is to advise that a fax has been received in error:

Sender: [name and job title]

Date and time received: [date and time]

Subject of fax: [include subject but no further detail or identifiable information]

Please could we ask that in future fax numbers are checked by calling ahead prior to sending to ensure that this incident is not repeated and information is sent to the correct recipient.

We will not attempt to forward the fax received to the correct recipient and will destroy the fax in a confidential manner.

An internal incident has been logged and should this be a regular occurrence then the organisation will formally escalate this to gain a resolution.

APPENDIX H - INFORMATION GOVERNANCE TEAM CONTACT INFORMATION

CCG IG Lead

IGSO name and contact details –

Emma Styles

emma.styles@staffordshirecss.nhs.uk

Tel: 0300 404 2999 ext 8214
Mobile: 07825 716409

IG Manager –

Hayley Gidman

Hayley.gidman@nhs.net

APPENDIX I - INFORMATION GOVERNANCE POLICY AND INFORMATION GOVERNANCE HANDBOOK SIGN OFF FORM

Acknowledgement of your personal responsibility concerning security and confidentiality of information (relating to patients, staff and the organisation).

Personal Details	
Surname:	
Forename(s):	
Job Title:	
Department:	
Location:	

Declaration:

I can confirm that I have read and understood Dudley CCGs "*Information Governance Policy and Information Governance Handbook*"*.* I understand that I am bound by a duty of confidentiality and agree to adhere to the Information Governance Policy and Handbook at all times.

Signed:

Date:

APPENDIX J - CONTRACT, TEMPORARY AND WORK PLACEMENT STAFF CONFIDENTIALITY AND COMPLIANCE AGREEMENT

1. Confidentiality

1.1 In the course of your employment with Dudley CCG (“the CCG”) you will receive and acquire confidential person/patient identifiable and commercially sensitive information that is the property of the CCG.

1.2 During and after your employment with the CCG **you must** take all reasonable steps to ensure the confidentiality of information that has been disclosed to or obtained by you is maintained.

1.3 You must not, either during or after your employment with the CCG:

- Disclose any person identifiable or confidential information relating to the business or affairs of the CCG, its service users or associated entities unless specifically authorised to do so in writing.
- Other than to the extent that is necessary to enable you to perform your duties:

  i. make extracts from, copy or duplicate confidential information;

  ii. make adaptations of confidential information;

  iii. make use of confidential information for private purposes, or in any manner which may, or is calculated to cause injury or loss to the CCG, its service users, customers or associated entities; and

  iv. other than for the benefit of the CCG make notes, documents, working papers or memorandum relating to any matter within scope of the business of the CCG or concerning any of its dealings or affairs.

1.4 Clauses 1.2 and 1.3 shall continue to apply despite the termination or cessation of your employment by either the CCG or you.

1.5 Without limiting the generality of the above, for the purpose of this clause, “confidential information” means and includes any information relating to the CCG, its business and activity including but not limited to person and patient identifiable information and other sensitive information in whatever form but excluding any matter that has become public knowledge or part of the public domain and all other information provided to you which is either labelled or expressed to be confidential, or given to you in circumstances where one would expect the information to be confidential to the CCG.

2. Compliance

1.1 During your employment with the CCG it is a requirement that you comply with all relevant legislation. These shall include, but not be limited to:

a) The Data Protection Act 1998

b) The Human Rights Act 1998

c) The Crime and Disorder Act 1998

d) Common Law Duty of Confidentiality

e) Freedom of Information Act 2000

In addition to the above mentioned legislation, consideration may also need to be given to the following when sharing personal information:

a) The Caldicott Committee Report

b) The Regulation of Investigatory Powers Act 2000

c) Information Security Standard ISO 27001

1.2 You will ensure that you understand the relevant elements of the applicable legislation that applies to your role within the organisation and ensure that you comply with legislation when carrying out your role.

1.3 During your employment with the CCG you will be required to comply with all relevant policies that are currently in place that relate to the sharing of information and confidentiality.

1.4 You will undertake mandatory Information Governance e-learning, and any other training as required, within the timescales specified by the CCG for any new starters within the organisation.

3. Deletion of data on Cessation

3.1 Upon cessation of your employment, you are required to deliver to the CCG all copies of information, including person identifiable information that you have used in the course of your official duties and to undertake that you will not use any person identifiable information for any use having terminated your employment with the CCG. You must also return any associated removable media in your possession.

I undertake to comply with the above obligations and conditions as required by the CCG and as stated above to protect the organisations confidential information and all relevant compliance requirements.

Name: ____ *(Please print)*

Signature: ______________________________ *Date:* _______________________

APPENDIX K – LEAVERS AND MOVERS CHECK LIST

Name of Employee:

Job Title: **Leaving Date:**

Checklist completed by:

Name: **Job Title:**

Date:

<u>**IF USER IS LEAVING THE ORGANISATION**</u>	**Date / Call Reference**
NETWORK ACCOUNT: A call should be logged with the IT Service to advise of leaving date in order to have network account closed	
NHS.NET: A call should be logged with the IT Service to have their account marked as a leaver from your organisation	
SMARTCARD: RA02 should be completed to notify RA team of the roles to be removed	

<u>**IF USER IS MOVING WITHIN THE ORGANISATION**</u>	**Date / Call Reference**
NETWORK ACCOUNT: A call should be logged with the IT Service to advise of relevant changes to job title etc	
SMARTCARD: RA02 should be completed to notify RA team of the roles to be amended	
SHARED FOLDER ACCESS: Review existing shared folder access and arrange to be amended as necessary	