NHS
Bradford and Airedale

NHS

Bradford and Airedale
Community Health Services

Information Governance User Handbook

Bradford and Airedale NHS
NHS Bradford and Airedale Community Health Services

Better information,
better health

CONTENTS

1.0 Introduction

1.1 Information governance

'Information governance is a framework for handling information in a confidential and secure manner, to appropriate ethical and quality standards, in a modern health service'

Information governance ensures necessary safeguards for an appropriate use of patient, personal and business sensitive information. Key areas are information policy for health and social care, information governance standards for the National Programme for IT systems and development of guidance for the NHS and partner organisations.

Information governance sits alongside clinical governance, research governance and corporate governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It provides a consistent way for staff to deal with the many different information-handling requirements, initially including:

- Information governance management
- Confidentiality and data protection assurance
- Information security assurance
- Clinical information assurance
- Corporate information assurance.

All staff need to learn about information governance to help ensure that they follow the best practice guidelines on information handling to enable them to manage information for the benefit of the patient or client. Patients and clients will know that their information will not be disclosed or used inappropriately.

1.2 How this guidance will help you

This user handbook gives you a brief introduction to information governance and summarises the key user procedures that have been developed to support the organisation's information governance policies.

The aim of this booklet is to ensure that you are aware of your roles and responsibilities for information governance. You must sign a declaration to confirm that you have received the booklet and that you are aware it is your responsibility to read and understand it.

Your signed declaration must be sent to the HR support team where it will be placed in your personnel file.

It is your responsibility to ensure that you read the associated policies and procedures, which are available on the organisations extranet site.

For a full list of all policies and procedures and details of the link to the extranet see page [37]

Remember…

everyone is responsible for

information governance

2.0 Information governance policy statement

Objective

The objective of information governance is to maximise the value of organisational assets by ensuring that data is:

- held securely and confidentially
- obtained fairly and lawfully
- recorded accurately and reliably
- used effectively and ethically
- shared and disclosed appropriately and lawfully.

Policy

The purpose of the policy is to protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.

It is the policy of the organisation to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- information will be supported by the highest quality data
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- information security training will be available to all staff
- all breaches of information security, actual or suspected, will be reported to, and investigated by the information governance manager
- the user procedures support the policies and apply to the organisations, and all its staff, agency staff, seconded staff and contractors.

2.1 Organisational responsibilities

Chief Executive - has board level responsibility for ensuring an effective policy for information governance is in place within the organisation.

Caldicott Guardian (CG) - ensures that the Trust has the highest practical standards for handling patient identifiable information and acts as the 'conscience' of the Trust. The CG facilitates and enables information sharing and advises on options for lawful and ethical processing of information.

Senior Information Risk Owner (SIRO) - working within a simple governance structure, with clear lines of ownership and well defined roles and responsibilities, the SIRO will provide an essential role in ensuring the identified information security threats are followed up and incidents managed. The SIRO will also ensure that the board and the accountable officer are kept up-to-date on all information risk issues. The role will be supported by the organisation's information governance manager, the risk manager and the Caldicott Guardian, although ownership of the information risk policy and risk assessment process will remain with the SIRO.

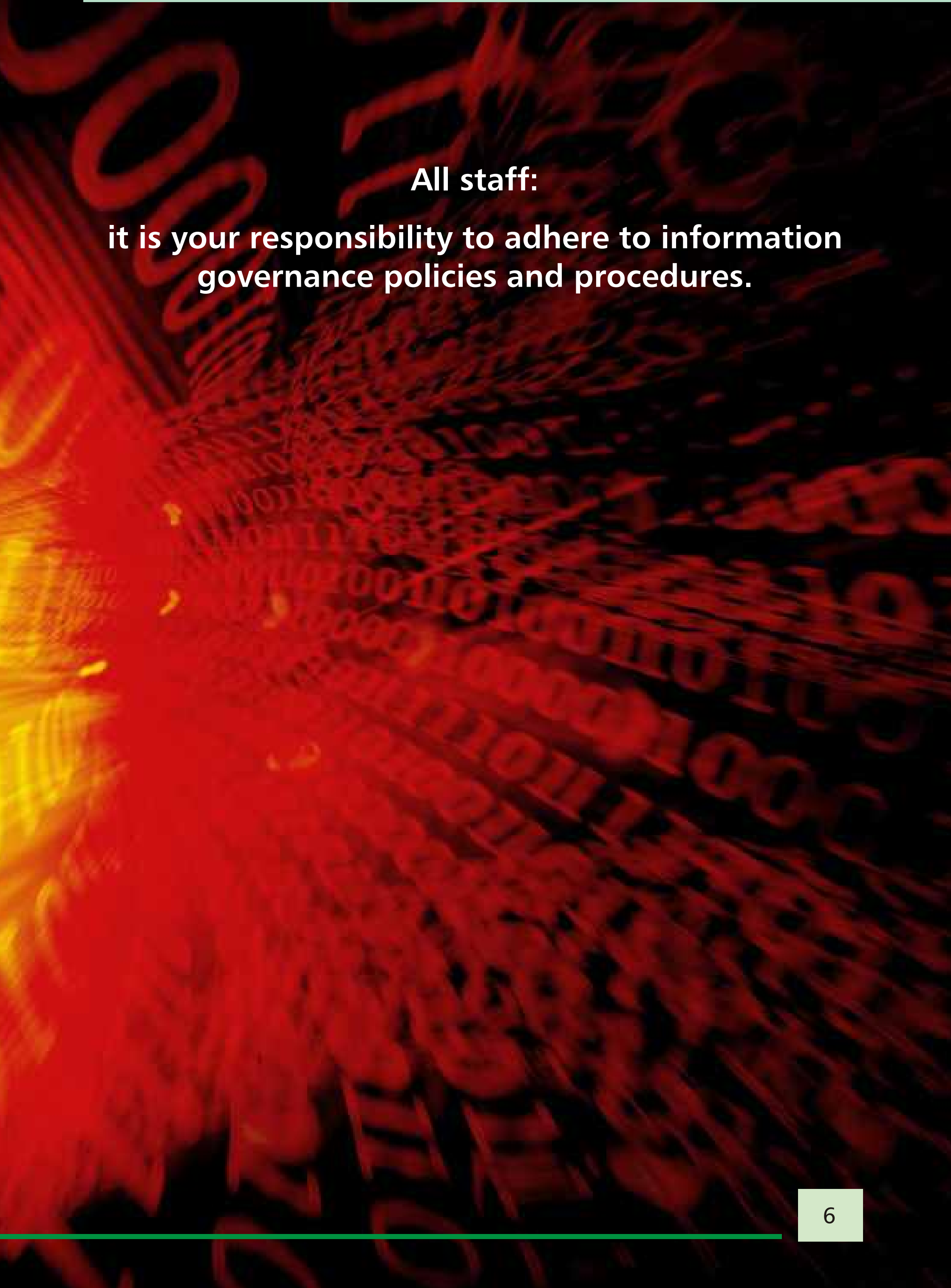
Information Asset Owner (IAO) - owners of one or more information assets, they will lead and foster a culture that values and protects information. The IAO will understand and address risks to information assets and provide assurance to the SIRO.

Information Asset Administrators (IAA) – provide support to their IAO by

- ensuring that policies and procedures are followed
- recognising potential or actual security incidents
- consulting their IAO on incident management
- ensuring information asset registers are accurate and up-to-date

Information governance manager - has responsibility to maintain an awareness of information governance issues within the organisation, review and update the information governance policies and audit procedures relating to the policies where appropriate on an ad-hoc basis.

Line managers - will take responsibility, ensuring that the information governance policies are implemented within their group or department.



All staff:

it is your responsibility to adhere to information governance policies and procedures.

3.0 Confidentiality

Everyone working for the NHS is under a legal duty to keep patient information confidential. This is written into all NHS employment contracts. External agencies, third parties and contractors have to understand and sign a confidentiality contract. What they see or hear stays with them. A breach of confidentiality directly or indirectly is a disciplinary offence, which could result in dismissal and/or prosecution. **This includes accessing records about yourself, family or friends that you have no legitimate reason to access.**

The organisation has a confidentiality code of conduct which all staff are expected to follow and which is available on the information governance website.

3.1 Caldicott

A Caldicott Guardian is appointed by each NHS organisation. It is their duty to ensure that patient data is kept secure and that all data flows, both internal and external, are periodically checked against the Caldicott principles.

- Justify the purpose(s)
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law.

Board appointed Caldicott Guardians will make decisions for the organisation on how, what, when and why patient identifiable information will be used by the organisation and how it will be received or sent by the organisation.

The commissioning Caldicott Guardian is Anita Parkin, director of public health

The provider services Caldicott Guardian is Margaret Waugh, head of programmes and estates

3.2 Legitimate access to patient information and the NHS Care Record Guarantee.

All staff should be aware that any access made to electronic records is auditable and that audits are run periodically to check that any access made is legitimate and required as part of a patients healthcare pathway.

The NHS Care Record Guarantee provides patients with information on their rights to see and obtain copies of their records as well as being able to request a list of everyone who has accessed their record. Patients can also ask to place restrictions on who may have access to their records, if they have any concerns.

It is extremely important that you only access information relating to the patients you are delivering care to. **You should never access your own record, or that of a friend or family member.**

Anyone found to be accessing information which they can not justify their legitimate need to, may be subject to disciplinary action, including dismissal in accordance with the organisations disciplinary procedures.

3.3 Sharing information

Information that can identify individual patients must not be used or disclosed for any other purpose than healthcare, unless the individual patient or patients have given their explicit consent or there are legal reasons.

The organisation has adopted the **NHS Confidentiality Code of Practice** and all staff should adhere to the guidance. A copy of the guidance has been placed on the organisations's intranet site on the Information Governance pages. The guidance provides advice on using and disclosing confidential patient information and has models for confidentiality decisions.

An overarching **information sharing protocol** has been developed for the Bradford and Airedale NHS Health Partnership. The protocol provides rules and procedures for the sharing of patient information between different organisations (available on the information governance pages of the intranet under confidentiality).

4.0 Information governance key user procedures

4.1 Human resources security

DO ✓

- Be aware of your responsibilities for information security (see information governance procedures 'roles and responsibilities for information security' on the extranet)
- Remember that you have signed a confidentiality agreement within your contract of employment
- Be aware that unauthorised disclosure or misuse of personal data will be treated as a serious disciplinary offence
- Ensure that temporary staff and third party contractors sign a confidentiality agreement available from the HR department or the information governance team
- Be aware of information governance policies and procedures – available on the information governance website
- Ensure that you receive appropriate training to enable you to carry out your work efficiently
- Ensure that your training needs are assessed on a regular basis
- Know how to report security incidents (see 'How to report an information security incident' on page 35)
- Be aware that the organisation has a formal disciplinary process for dealing with staff that violate the organisations' policies and procedures.

DO NOT ✗

- **Attempt to prove a suspected security weakness, as testing a weakness might be interpreted as potential misuse of the system**
- **Allow third parties access to the organisation's hardware, without correct authorisation**
- ***Ignore security incidents!***

4.2 Physical security

DO ✓

- Report the loss of your access card immediately to the building custodian/estates manager
- Protect your smartcard as if it were your credit card
- Ensure all IT equipment is reasonably protected against theft and unauthorised access
- **Follow the procedures for use of portable it devices, mobile phones and removable media and ensure that blackberry's are password protected**
- Ensure that assets are disposed of in accordance with the organisations's procedures
- Wear ID badges
- Ensure that visitors sign a visitors book and receive a visitors ID badge
- Challenge unidentified visitors in a controlled area
- Escort visitors in secure areas at all times
- Operate a clear desk and clear screen policy
- Ensure confidential and patient information is locked away when not required
- Ensure that confidential waste is stored securely, prior to disposal
- Ensure incoming and outgoing mail points are in secure areas
- Clear confidential and patient information away from printers and fax machines immediately
- Ensure password protected screensavers are be installed on all PCs (where possible)
- Ensure PCs are not left logged on and unattended - Ctrl-Alt-Delete, Lock Workstation
- Ensure keys to premises are securely stored
- Ensure that secure areas are kept secure and locked when not in use
- Site computer screens away from unauthorised viewing
- Ensure that all deliveries are correctly checked, recorded and distributed in a secure manner.

DO NOT ✗

- **Take the organisations's equipment, information or software off-site without authorisation.**
- **Leave equipment unsecured in public areas**
- **Tell others what keys you have been entrusted with**
- **Disclose the codes for security keypad locks**
- **Do not leave your smartcard in your pc unattended or allow others to use it.**

4.3 Use of Portable IT Devices

Portable devices include laptops, notebooks, tablet computers, PDA's, blackberrys and mobile phones.

DO ✓

- Store portable equipment securely when not in use on site and off site
- Ensure files containing personal or confidential data are adequately protected e.g. encrypted and password protected (with a minimum password length of 6 characters)
- Ensure that PDA's/Blackberrys' are configured so that they lock after a maximum period of 5 minutes inactivity. Once locked the PDA/Blackberry should be set to require password authentication to resume use
- Install password protected screensavers on laptops
- Use and regularly update anti-virus software
- Take regular backups of the data stored on the portable equipment
- Ensure a nominated person is responsible for each portable device
- Maintain a register where portable equipment is used in a pool to enable identification of current user
- Obtain authorisation prior to the removal of portable equipment from the premises
- Be aware that software and any data files created by staff on Trust portable computer devices are the property of the Trust
- Report **immediately** any stolen portable equipment to the police and line manager (failure to report a stolen mobile phone could result in significant charges)
- Be aware that the security of your portable computer device is your responsibility and you should check your home and car insurance policies to ensure they cover for business use
- Ensure that portable devices are returned to the Trust if you are leaving employment (**A final salary deduction may be made if equipment is not returned**)
- Log your laptop on to the Trusts network at least once every 3 months to ensure that the encryption password remains valid.

DO NOT

- Store person identifiable information on removable equipment unless it is absolutely necessary and then ensure that it is encrypted/password protected
- Use your own portable computer device or digital storage device such as flash cards, USB memory sticks and portable hard drives for Trust business
- Leave portable equipment in places where anyone can easily steal them
- Leave portable equipment visible in the car when traveling between locations
- Leave portable equipment in an unattended car
- Leave portable equipment unattended in a public place
- Install unauthorised software or download software / data from the internet
- Disable the virus protection software
- Use portable computer devices outside the Trust premises without line manager authorisation
- Allow unauthorised personnel/friends/relatives to use portable equipment in your charge
- Connect any unauthorised equipment to the network e.g. personal iPhones, mp3 players, wireless routers etc - if in doubt contact IT service desk.
- Take person identifiable information off site without authorisation from your Line Manager

4.4 Environmental security

DO ✓

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

DO NOT ✗

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

4.5 Protection against malicious software

DO ✓

- Ensure that anti-virus software is operating and is up to date. To do this right click on the McAfee virus shield icon and select 'about'. If the date is more than a week old then contact IT Service Desk on 01274 237777
- Update virus checking software regularly on laptops by logging onto the organisation's network
- Ensure that all files on electronic media of uncertain origin are virus checked before being loaded onto the network
- On discovering a virus:
  - note any symptoms
  - immediately shut down PC
  - do not use infected media on another PC
  - report it immediately to the IT Service Desk on 01274 237777
  - ensure that all other possibly infected equipment is isolated
  - Use write-protected disks and tapes where possible.

DO NOT ✗

- **Remove or disable anti-virus software from a PC**
- **Change the way anti-virus software is configured**
- **Load unauthorised software including screensavers/games**
- **Use unauthorised software on the organisation's equipment**
- **Attempt to 'clear' an infected PC**
- **Open email with suspicious attachments; contact IT Service Desk for guidance**
- **Accept any freeware advertised as it may contain spyware/adware, software used to gather information about you and the organisation.**

4.6 User access control and password management

DO ✓

- Ensure that a user ID and password is required for access to the network and any applications containing personal information (see network access procedures available on the information governance pages of the intranet)
- Ensure that you read and follow the declarations set out in the RA01 short form conditions if you are a smartcard user
- Be aware that NHS CRS smartcards help control who accesses what and at what level. Using the same technology as chip and pin, members of staff are identified by names, by photograph and a unique identity number
- Select quality passwords with a minimum of six characters which are:
  - easy to remember
  - not based on anything somebody else could easily guess, eg: names, telephone numbers etc
  - a combination of letters and numbers
- Avoid re-using or recycling old passwords
- Keep passwords confidential - you are responsible for information entered using your password. Failure to protect your password or workstation could result in disciplinary action
- Change passwords at regular intervals, and also if there is any indication of a possible system or password compromise
- Use password protected screensavers when away from your desk (activated by - Ctrl+Alt+Delete + lock workstation)
- Be aware that you are responsible for any activity performed under your logon ID and password. This includes any activity undertaken by someone else while your PC is left logged in and unattended without a password-protected screensaver
- Ensure that you log off correctly, ie: don't just switch the machine off, exit properly
- Be a responsible manager and terminate your staff network access or smartcard access rights when they leave your team/unit.

DO NOT

- Leave a PC logged in and unattended (unless protected by a password screensaver)
- Use someone else's ID or password to access the network or clinical system
- Write a password down, unless stored securely
- Give your user id and password to anyone else e.g. for a new/ temp user

4.7 Exchanges of information and software

DO ✓

- Be aware of safe haven guidelines for confidential information, e.g. faxes
  - Telephone the recipient and ask them to wait by the fax machine whilst you send the document
  - Ask them to acknowledge receipt
  - Check the number dialled, and check again before sending
  - Where possible use pre-stored numbers
  - Send a test fax first
- Take care when making a phone call to make sure that you do not reveal confidential information, e.g. by being overheard
- Take care when listening to answer phone messages, e.g. close the door when retrieving messages
- Adhere to the text messaging procedures (see extranet). In particular, ensure that patients are fully informed of the risks and obtain their consent to the process (This should be evidenced either in writing using a signed consent form or noted on the clinical system) **Note : providing a mobile phone number does not constitute consent to use the number for text messaging.**
- Follow the patch-wide information sharing protocol available on the information governance pages of the intranet
- Adhere to the procedures for confidentiality (see page 32 for more details)
- ‘Ensure that envelopes containing personal identifiable information (PII) sent via **internal or external** mail are clearly and correctly addressed, marked ‘confidential’ and the senders addressincluded’. (**Never send** PII relating to more than 20 patients in one envelope).
- Adhere to the Personal information in transit procedures (see extranet) e.g.
  - Remember that you are responsible for what happens to this information in transit and until it has been returned to its safe store or is destroyed or disposed of correctly
  - Always check where you were sitting to ensure you have gathered all information before leaving a client, a meeting, the bus, taxi, train or plane ……
  - Consider whether you really need all the information. Take only the minimum amount of information to support the work that is to be done

DO NOT

- Leave confidential messages on answering machines
- Leave confidential information on white boards
- Leave confidential information in message books
- Have confidential conversations in public places or open offices or meeting places with thin walls
- Disclose sensitive or personal information to anyone on the phone or via fax, unless you are sure they are who they say they are and that they need to know those details
- Send PII via internal mail using a transit envelope
- Send clinical/personal information via text messages
- Keep sending copies of documents to a variety of printers if it does not print out immediately and if there is a problem check your printer 'set up'
- Leave without checking you have everything
- Leave personal identifiable information visible in an unattended car
- Pass information/data (especially Personal Identifiable Information) to anyone who does not have a legitimate right to it just because you hold a copy e.g spreadsheets of data

4.8 Email security

DO ✓

- Be aware that the email system is primarily for business use. Occasional and reasonable personal use is permitted provided that it does not interfere with the performance of your duties and does not conflict with the organisations' policies
- Be aware that the organisation may inspect email addresses and contents (including personal email) without notice
- Follow the email procedures for email etiquette and best practice, acceptable use and the retention of messages (see extranet)
- Be aware that the same laws apply to email as to any other written document
- Keep the amount of email in your inbox to a minimum
- Use an auto signature which must include your contact details e.g telephone number and work address
- Be careful about content - email is easily forwarded
- Check your inbox regularly
- Use out of office assistant to advise people when you are not available
- When required, ensure email delegates are set up appropriately, to allow access to your emails whilst out of the office, on holiday etc
- Use the address book (or contacts) where possible, to prevent incorrect addressing
- Be aware that you do not own the documents that you or your colleagues create, and you do not have intellectual property rights over them
- Report to the information governance team any email that you receive, or become aware of, that may be regarded as illegal or offensive
- Be aware that your mailbox may be opened to access information if absent, eg: sickness or holiday
- Remove any personal contents from your mailbox and personal network folders when leaving employment; (it may be made available to a replacement or line manager)
- Follow the guide to winzipping and encrypting documents, available on the information governance pages of the intranet
- Be careful when sending work related photos, pictures / logos etc – check file size (see guidance on the IG website)

DO NOT

- Send patient or sensitive data via email unless absolutely necessary and if so a risk assessment should be undertaken, confidential/sensitive data must be encrypted and winzipped
- Leave email logged in and unattended
- Speak to the media, analysts or to the public on behalf of the organisation via email unless you are duly authorised to do so
- Use email to set up, maintain or promote personal business
- Send email that is or could be considered to be sexually or racially offensive, pornographic, defamatory, abusive, profane, criminal or for any other unauthorised purpose
- Use email for commercial activities or to advertise goods
- Create or forward chain mail
- Create auto-forwards of emails to home or other personal email addresses
- Send to large numbers of people unless you are sure it is directly relevant to their job - spamming is not permitted
- Attach large files to emails(10mb+) - where possible send a link to the file or winzip it to reduce its size

4.9 Internet security

DO ✓

- Be aware that the internet and intranet is primarily for business use Occasional and reasonable personal use is permitted e.g. during lunch breaks, provided that it does not interfere with the performance of your duties and does not conflict with the organisations' policies
- Follow the procedures for internet use (see extranet)
- Be aware the same laws apply to internet communications as for written documents
- Remember that the organisation will use monitoring and filtering software to prevent access to sites which are not work related or may have offensive or illegal content
- Remember that the organisation will undertake audits to monitor usage of the internet to ensure that it is not being used inappropriately
- Be aware that inappropriate use may result in prosecution and/or disciplinary action
- Be aware of the Social media procedures (see extranet) e.g. obtain approval from your line manager for any online activities associated with work for the Trust e.g. by displaying an @bradford.nhs.uk or nhs.uk e-mail address, by joining the NHS network or Trust-related networks on social network sites or by making reference to the Trust as your employer
- Be aware of spyware and adware software programs that surreptitiously monitor your actions. This software is used to invade your privacy gathering data about you and your organisation, often bombarding systems with pop-up ads, causing countless problems to networks

If you are offered something for nothing in an advert, you could be getting far more than you bargained for!

Don't click

DO NOT

- Leave the internet logged in and unattended – you are responsible for what happens under your login
- View, download, transmit or archive any information, graphics, pictures, music, video clips unless it is relevant to your work area and NEVER download any that are defamatory, obscene, racist, sexual, or of a criminal nature
- Load executable programs or applications from the internet, this includes software and shareware
- Set up, maintain or promote personal business for commercial activities or to advertise goods or services
- Speak on behalf of the organisation in newsgroups or chat rooms
- Use the internet and web access in a manner that breaks any of the organisations' policies
- Use the Trust logo on personal web pages
- Reveal confidential information about our patients, staff, or the Trust. Never post any information that can be used to identify a patient's identity or health condition in any way. Protecting patient confidentiality and patient health information is everyone's number one responsibility.

4.10 Information Risk

Information Asset Owners (IAO's) have been identified for the Trust's information assets e.g. databases, system documents and procedures, archive media/data, paper records etc.

IAO's are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. IAO's may be assisted in their roles by staff acting as Information Asset Administrators who have day to day responsibility for management of information risks affecting one or more assets.

For further information see the Information Risk Policy on the Extranet.

DO ✓

- Ensure any new information asset is added to the Trust's Asset Register (contact the IG team)
- Ensure the IG team are contacted if any new system, project or process involves a new use of personal information or significantly changes the way it is handled (to ensure a Privacy Impact Assessment is considered)
- Ensure a system specific security policy is documented for any system that contains personal information (see information risk assessment and management procedure on extranet)

NHSBA SIRO is Steve Ingleson – director of performance management

BACHS SIRO is Margaret Waugh – head of programmes and estates

DO NOT ✗

- **Develop a database containing identifiable information without consulting IG team or systems development team**

4.11 Compliance requirements

DO ✓

- Be aware that the organisation is obliged to abide by all relevant European Union legislation.
- Be aware of the following legislation:
  - Data Protection Act 1998 (see DPA procedures on extranet)
  - Freedom of Information Act 2000 (see FOI procedures on extranet)
  - Access to Health Records Act 1990
  - Copyright, Designs and Patents Act 1988
  - The Computer Misuse Act 1990
  - Human Rights Act 1998
- Follow the Caldicott principles (see Caldicott guidelines on page 32)
- Be aware that all staff are responsible for information security
- Ensure you know who to forward a request to when access to health records or a freedom of information request is received (see page 27: information governance team)

DO NOT ✗

- **Breach legal requirements**
- **Be ignorant of the legal requirements that affect you**
- **Copy software illegally**
- **Breach copyright laws**

4.11.1 Data Protection Act (DPA) Policy

The organisation needs to collect personal information about people who it deals with so it can carry out its business and provide services.

Such people include patients, staff (present, past and prospective), suppliers and other business contacts. No matter how it is collected, recorded and used – eg: on a computer or on paper - personal information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1998.

The lawful and proper treatment of personal information by the organisation is extremely important. The success of our business and the confidence of our service users and staff is achieved by everyone knowing their roles and responsibilities. We ensure that the organisation treats personal information lawfully and correctly.

The organisation fully supports and complies with the eight principles of the Act

Personal data must:

- **Be processed fairly and lawfully**
- **Be obtained or processed for specific lawful purposes**
- **Be adequate, relevant and not excessive**
- **Be accurate and kept up to date**
- **Not be kept for longer than necessary**
- **Be processed in accordance with rights of data subjects**
- **Be kept secure**
- **Not be transferred outside the European Economic Area (EEA) unless there is adequate protection**

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

All staff will:

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
- Understand and comply with the eight DPA principles
- On receipt of a subject access request from an individual for information held about them, immediately notify their line manager and the information governance team
- Inform the IG team if any personal information is to be transferred outside the European Economic Area (EEA)

The organisation will:

- Provide training for all staff who handle personal information
- Carry out regular checks to monitor and assess processing of personal data to ensure the organisations's DPA notification is kept up to date
- Develop and maintain DPA procedures to include roles and responsibilities, notification, subject access, training and compliance testing

The organisations' data protection lead is Bonnie Hartley, tel: 01274 237305

4.11.2 Freedom of Information (FOI) Policy

The Freedom of Information (FOI) Act was passed in 2000 and replaces the Open Government Code of Practice that has been in place since 1994. The Act gives the public a general right of access to all types of recorded information held by public authorities.

The Act places a statutory obligation on all public bodies to publish details of all recorded information that they hold and to allow, with a few exceptions, the general public to have access to this information on request.

The organisation recognises the importance of the Act and will ensure that appropriate systems are put in place to publicise what recorded information is kept by the organisation and how this information can be accessed on request by the general public. The overall responsibility for this policy is with the chief executive.

All staff will, through appropriate training and responsible management:

- Observe all forms of guidance, codes of practice and procedures about the storage, closure, retention and disposal of documents and records
- Be aware that ultimately the general public may have access to any piece of information held within the organisation and must pay due regard to how they record information as part of their normal duties
- On receipt of an information request, immediately notify the FOI lead
- **Provide information promptly when requested by the FOI lead (the organisation has only 20 working days to respond to a request).**
- Be aware that the organisation may receive requests about employees (i.e. salary banding) and we may have to release information which is relevant to their role. We will not release information classed as personal 'sensitive' information, i.e. information which does not relate to your role.

The organisation will:

- Maintain and publish a publication scheme
- Provide all staff with an introductory briefing on the FOI Act and related procedures
- Develop and maintain clear procedures for recognising and responding to requests for information under FOI
- Develop and maintain a comprehensive record management strategy that supports FOI.

Bradford and Airedale NHS
Bradford and Airedale Community Health Services NHS

The organisations' FOI lead is Barbara Booth, tel: 01274 237508

4.11.3 Environmental Information Regulations

Like Freedom of Information anyone can make a request for information but under Environmental Information Regulations (EIR) these requests can be made verbally or in writing but have to be replied to in writing. The organisation must to respond to EIR requests within 20 working days.

Environmental information is divided into the following six main areas (as stated on the Information Commissioner's website):The state of the elements of the environment, such as air, water, soil, land, fauna (including human beings) Emissions and discharges, noise, energy, radiation, waste and other such substances

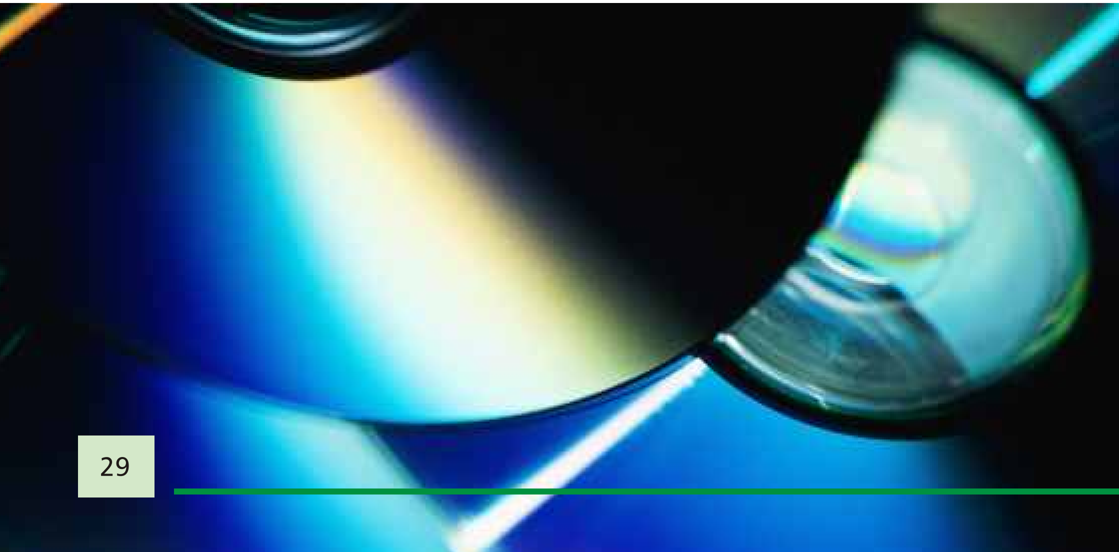
- Measures and activities such as policies, plans, and agreements affecting or likely to affect the state of the elements of the environment
- Reports, cost-benefit and economic analyses
- The state of human health and safety, contamination of the food chain
- Cultural sites and built structures (to the extent they may be affected by the state of the elements of the environment).

If you receive a request for information under EIR then inform the FOI lead, Barbara Booth immediately.

4.11.4 Software, data and media management

DO ✓

- Be aware that shareware, freeware and evaluation software is bound by the same policies and procedures as all software. Advice must be sought from the IT Service Desk if you require this type of software
- Be aware that the software policies apply to laptop and hand-held devices as well as desktops
- Be aware that the organisation forbids the use of any software that does not have a licence, and anyone found to be using, or in possession of, unlicensed software will be subject to disciplinary procedures
- Respect all computer software copyrights and adhere to the terms and conditions of any licence to which the organisation is a party
- Actively and frequently undertake housekeeping of your data, eg: delete unwanted files regularly as information is soon out of date.
- Ensure that all disks and tapes are suitably labelled, i.e: so that the contents are not easily identified
- Archive files and documents on a regular basis - delete documents you don't need anymore in line with the retention schedule policy available in the records management policy on the intranet
- Ensure that tapes and disks are disposed of securely, eg: in a shredder or confidential waste
- Clear all patient or confidential information off disks and tapes by reformatting - not by deletion - before disposing of them



DO NOT

- Install software without authorisation including freeware, shareware, trial software
- Install non-business software eg: games, unless authorised to do so
- Copy software from the organisations' systems onto your own PC, eg: at home
- Store personal data on the organisations' systems, eg: photographs, music files, videos
- Take a copy of Trust information for use off site unless authorised to do so by your line manager
- Store information/data for any longer than is absolutely necessary
- Store any documents on 'c' drive or local hard drives
- Dispose of disks and tapes without erasing data
- Forget to set the write protect on disks and tapes
- Misuse disks and tapes; exposure to heat will damage the surface and the data

Remember

All PCs are actively monitored and audited. Any unauthorised software will be detected

4.12 Records Management Policy

DO ✓

- Be aware of the records management policy and procedures and ensure that you:
    - Know the retention times for records (refer to the NHS Records Management Code of Practice)
    - Follow the corporate filing structure when creating records
    - Ensure records are disposed of appropriately
    - Know who your local records manager is.
- Be factual, consistent and accurate, for example: ensure records are:
    - Written as soon as possible after an event has occurred
    - Written clearly, legibly and in such a way that they cannot be erased
    - Readable on any photocopies
    - Clear, unambiguous, and concise (where possible)
    - Written in terms that the patient/service user can understand.
- Be aware that patients have a right to view and have copies of their information so anything which has been recorded about them may well be provided to them

For clinical records:

- Provide evidence of the care planned, the decisions made, the care delivered and the information shared
- Provide evidence of actions agreed with the patient (including consent to treatment and/or consent to share).

Ensure manual records are:

- Formally booked out from their normal filing system
- Tracked if transferred, with a note made or sent to the filing location of the transfer
- Returned to the filing location as soon as possible after completion of treatment
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently
- Stored closed when not in use so that contents are not seen accidentally
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons
- Held in secure storage with clear labeling indicating sensitivity and permitted access

DO NOT

- Use unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation or offensive subjective statements
- Record personal opinions/comments regarding a patient (restrict to professional judgment on clinical matters)
- Leave sensitive or confidential information where it can be accessed inappropriately
- Store information/data for any longer than is absolutely necessary

5.0 Home working

The purpose of this policy is to provide all staff with clear information regarding home working, either on an occasional basis, or permanent arrangement

DO ✓

- Obtain authorisation prior to working from home (see home working procedures available on the Human Resources policies pages on the extranet)
- Ensure that updated anti-virus software is used
- Ensure that any equipment supplied by the organisation is used only by you, for authorised work only
- Ensure that a risk assessment is undertaken if you need to use confidential information at home. (Seek advice from the information governance team).
- Be aware that your legal duty to maintain confidentiality relates to data taken home
- Follow the procedures for the use of portable computer devices, mobile phones and removable media
- Be aware that you use your own PC at your own risk. The organisation will not be responsible for fixing faults etc
- Take regular data backups and ensure that they are stored, and transported, securely
- Be aware that it is your responsibility to ensure that you work in a suitable environment (health and safety). If in doubt, please speak to your health and safety advisor

Ensure that all confidential and sensitive data is removed from your PC before disposal or giving to someone else - contact IT Service Desk on 01274 237777 for advice

DO NOT ✗

- **Email confidential data to or from a home PC unless a risk assessment has been undertaken**
- **Email confidential data unless it is winzipped and encrypted (see guidance on the information governance pages of the intranet).**

6.0 How to report an information security incident

A security incident is any event, which has resulted in, or could result in:

- The loss, theft or disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or data being put at risk
- An adverse event, for example:
- Embarrassment to the NHS
- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss - for any suspected fraud - refer to the counter fraud policy on the intranet
- Disruption of activities.

All incidents, or information indicating a suspected incident should be reported as soon as possible, within two working days, to your line manager. Details of incidents must be reported via the organisations' risk incident reporting procedure using PRISM (process for risk management). The system allows us to collate information about the number of incidents being recorded across the district. By looking in detail at the collected information we can learn from things that go wrong and work to make it a safer place for both our patients and our staff.

The incidents should be reported using category 'patient safety-confidentiality' or 'Information Governance'. The Information Governance Manager is alerted to these incidents and will support the investigation being undertaken by the incident manager where appropriate.

Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as a serious untoward incident (SUI). All SUIs must be discussed within one working day with the Information Governance Manager and the Integrated Risk Team (NHSBA) or Head of Programmes (BACHS).

For further details please see the information security incident reporting procedure available on the extranet

Anything where there is a chance of harm or where harm has occurred must be reported.

For more information please contact;
Diane Netherwood, risk manager, 01274 237438.

7.0 Information governance team

You can obtain further information on any aspect of information governance from the following:

Information governance manager: Carol Mitchell

tel: 01274 237507 email: carol.mitchell@bradford.nhs.uk

Data protection (including access to health record requests) and Records management

Information governance co-ordinator: Bonnie Hartley

tel: 01274 237305 email: bonnie.hartley@bradford.nhs.uk

Freedom of information

Information governance specialist: Barbara Booth

tel: 01274 237508 email: barbara.booth@bradford.nhs.uk

Information governance toolkit for general practices, dentists, opticians and pharmacists

Information governance specialist: Wendy Harrison

tel: 01274 237728 email: wendy.harrison2@bradford.nhs.uk

Information governance privacy alerts

Information governance support and privacy officer: Taahir Rawat

Tel: 01274 256089 email: taahir.rawat@bradford.nhs.uk

8.0 Copy of your declaration

I confirm that I have received the following booklet and leaflet, understand that it is my responsibility to read and understand them, and to raise any queries or concerns with my line manager.

Information governance user handbook

A leaflet for staff about handling patient information

This booklet and leaflet have been developed to ensure that users are compliant with, but not limited to, the Data Protection Act (DPA) 1998, Freedom of Information Act 2000, Human Rights Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patent Act 1988 ISO27001 (formerly BS7799) and the Caldicott principles.

It is important to remember that you are accountable for your computer login and that all activity is auditable. It is your responsibility to ensure that only you know your password and that if you leave your PC logged in and unattended you must activate a password protected screensaver (press Ctrl + Alt + Delete, lock workstation) to stop any unauthorised use of your password and PC.

If you choose to make a note of any login IDs or passwords that you are using, lock them away in a secure place. Keep all passwords secure and do not disclose them to anyone.

You should be aware that inappropriate use, including any violation of this policy may result in the withdrawal of the facility and may result in prosecution and/or disciplinary action, including dismissal, in accordance with the organisations' disciplinary procedures.

Please note: a signed copy of your declaration will be placed in your personnel file.

9.0 List of Information governance policies and procedures

IG Policy	IG Procedure(s)
Organisation of information security	Roles and responsibilities for Information security
Human resources security (includes Third party confidentiality agreement form)	Information Security Incident reporting
Physical and environmental security	Use of portable equipment (Portable asset request form)
Operations management	
Network security	
Remote access	
Protection against malicious software	
Data backup, restore & file handling	
Exchanges of information	Personal identifiable information in transit Safe haven Text messaging Caldicott Confidentiality code of conduct Disclosures to police Access to records of deceased patients
Email Security	Email procedures
Internet Security	Internet procedures Social Media procedures
User Access Control	Network Access procedures
Home working	Home working procedures
Systems Development	Systems development procedure
Information Risk	Privacy Impact Assessments Information Risk Assessment and Management
Forensics Readiness	
Compliance requirements	
Software and data management	
Data protection	Data protection procedures Violent warning markers
Freedom of information and environmental information regulations	FOI & EIR procedures Round Robin procedures
Records management	Records management Local records management template Scanning records Audio and visual procedures

This list is not exhaustive and will be updated in line with policy/procedure reviews

The Information Governance Policies and Procedures are available on the Extranet at:

http://nww.bradford.nhs.uk/extranet/Policies/Pages/default.aspx
Link to IG website = http://nww.bradfordairedale-pct.nhs.uk/Information+governance/

10 IG - Top Ten ways to keep information secure!

Think about all information as if it contained your details!

1. **Lock your workstation:** When leaving your work station always **LOCK YOUR PC** – get into the habit of pressing **Control – Alt – Delete – Return**, whenever you leave your desk. Remember any work done under your log in will be attributable to you – even if you did not do it!
2. **Passwords: NEVER** share your login or password or use anyone else's login or password
3. **Smartcards: NEVER** leave your Smartcard unattended – **ALWAYS REMOVE IT** when leaving your workstation. As above - remember any work done under your log in will be attributable to you – even if you did not do it.
4. **Faxes:** When faxing personal or patient identifiable information always use a Safehaven fax machine. Full Safehaven procedures are available on the intranet.
5. **Emails: DO NOT** Send patient / sensitive data via email unless absolutely necessary and if so a risk assessment should be undertaken, data must be password protected and encrypted i.e. using WinZip. See the Information Governance, What's New page for instructions on how to winzip.
6. **Paper information:** Think about how you handle paper information as if it contained your own information e.g. diaries, patient lists, letters, would you leave your information on view for anyone to see – **ALWAYS** secure any information you are handling.
7. **Memory Sticks (USB's):** It is Trust policy that only Trust supplied encrypted memory sticks must be used for business purposes. Any existing Trust supplied unencrypted sticks or personal sticks must no longer be used.
8. **Laptops:** Every laptop must be encrypted with Safeboot software. (If you have a Trust issued laptop that is not encrypted please contact IT Service Desk immediately). The user id's and passwords for encryption are held on a central server and these details are downloaded to each laptop when it is connected to the network.

   You must remember to log your laptop into the network every 90 days otherwise the laptop will not work.
9. **IT Equipment:** DO NOT install unauthorised equipment onto your PC e.g. Wireless router, ipod, phone etc.
10. **Information Governance Training:** Information Governance Training is mandatory for all members of staff. Ensure you complete the **Introduction to Information Governance** mandatory IG training module on the NHS Connecting for Health Information Governance Training Tool, details available on the website.

    http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

NHS
Connecting for Health

Welcome to the Information Governance Training Tool

Why is Information Governance (IG) important?

Good Information Governance practice ensures necessary safeguards for, and appropriate use of, corporate, patient and personal information.

What is the purpose of the IG Training Tool?

The purpose of this tool is to ensure that IG training is available to all staff covering a range of training needs and learning competencies to support the implementation and development of an IG framework within an organisation. This site will be regularly updated and developed with additional materials, so watch out for new content.

Registered users log in here:

Username
Password

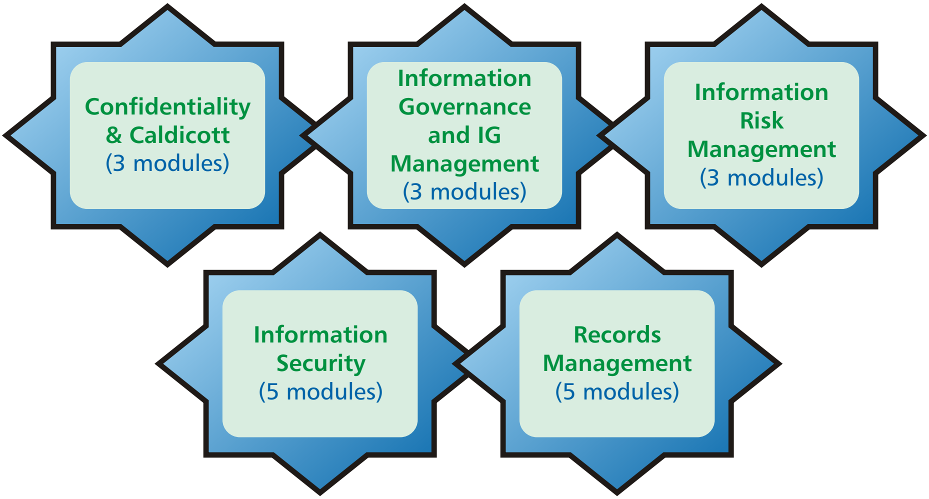
Login

› Problems logging in?

Mandatory requirement: ALL PCT and BACH's staff are required to complete the introduction to information governance module which can be found on the learning tools tab under :

⊞ Information Governance and IG Management (3 resources)

The IG Training Tool provides far more than just mandatory training. Once you have completed the mandatory module, expand your knowledge by undertaking further modules from the sections below:



Confidentiality & Caldicott (3 modules)

Information Governance and IG Management (3 modules)

Information Risk Management (3 modules)

Information Security (5 modules)

Records Management (5 modules)

www.igte-learning.connectingforhealth.nhs.uk

Published: 3rd Edition - November 2010 Revision date: November 2012
NHS Bradford and Airedale
Information governance team
email: Infogov@bradford.nhs.uk