Policy

Information governance and information security

Key messages

- All staff will receive information governance training on a yearly basis.
- The sharing of personal identifiable data by email, fax, post or telephone must comply with the safe haven procedures.
- Access to electronic systems must have the appropriate security measures in place such as user name access and passwords.
- All information must be held securely.

1 Scope

This policy applies to all Trust employees, including:

- staff who hold honorary contracts
- contractors working on behalf of the Trust
- the board of governors

2 Purpose

- To inform staff of their responsibilities in relation to information governance.
- To ensure compliance with the standards required in relation to information governance, including legal requirements.
- To embed the culture of information governance in the organization.
- To ensure there is effective control through adequate procedures and management practices over those resources which are required to provide information for the delivery of services.
- To ensure all of the Trust's information systems are secure and confidential.
- To ensure that confidentiality, integrity and availability of data are maintained.
- To ensure that there is a system of risk analysis in place to ensure all recognized threats are evaluated and that all preventative measures arising from all assessments of risk are examined for cost effectiveness and practical applications.

3 Definitions

Access profile: a template that describes permissions appropriate to a role or position.

Business Continuity Plan (BCP): this is a formal structured plan which describes how the business unit is to operate during a declared major incident.

BYOD: bring your own device.

BYOD container: The secure container hosts applications that require access to restricted corporate information and facilitates the clear separation of personal and corporate applications and any associated data on the mobile device. The container also provides in-transit and at-rest encryption of data.

CFH: Connecting for Health

CUH: Cambridge University Hospitals NHS Foundation Trust

Core operational network: part of the Trust's internal data network that provides controlled clinical and non clinical secure services.

End point protection software: software that controls various aspects of the use of PCs and other user devices.

FOI: freedom of information.

IAO: information asset owner

IGO: information governance owner

IGSG: information governance steering group

Information asset (IA): an information asset is an identifiable and definable information-based organisational component which is 'valuable' to the business of that organisation and without which critical business processes would potentially fail.

Information governance (IG): is a framework that ensures that personal and corporate information is dealt with legally, securely, efficiently and effectively to appropriate ethical and quality standards.

Information governance toolkit: enables organisations to measure their compliance with the information-handling requirements by assessing themselves against the following initiatives:

- information governance management
- confidentiality and data protection assurance
- information security assurance

- clinical information assurance
- secondary uses assurance
- corporate information assurance

Information risk assessment: the chance of something happening that involves information, which will have an impact upon the Trust's compliance with information governance requirements, the achievement of the Trust's objects and the provision of patient care.

Information system: includes manual files, electronic files, databases, applications and networks.

Linked accessible records and data repository (LARDR): The Trust's data warehouse system that holds historical patient data extracts from clinical systems no longer in use.

Mobile device: includes but is not limited to USB memory sticks, personal digital assistants (PDA), Blackberrys, laptops, net-books, CDs, external hard disks, tablet PCs, digital dictaphones, digital cameras, smart phones, mobile phones, data tapes, tape dictaphones, zip drives, z pens and memory cards.

New process: implementation of a new process that will have an impact on the way the Trust handles and uses personal identifiable information.

New system: implementation of a new or substantial upgrade to an IT system. Projects will be managed through the IT department's project process or via designated managers within departments.

Personal digital assistant (PDA): a hand held computer with data storage and processing functionality, but without direct access to the Internet or the mobile phone network.

Personal identifiable data (PID): this is data that may be used to identify an individual patient, staff member or other member of the public. For a more complete description, refer to the data protection policy and procedure.

Remote access: provision of access to the Trust's network services from non-Trust locations.

SIRO: senior information risk owner

Smart phone: a PDA with access to the Internet and mobile phone network.

Third party service provider/ data processor: Setting up a contract with an external supplier to either process personal data on the Trust's behalf or to provide a service to the Trust where they will require or have access to Trust information.

Trust data: recorded information in any media, which has been created or gathered as a result of any aspect of the work of all Trust employees. For further guidance please refer to the Trust data flow chart.

Trust-owned device: a device that has been purchased by the Trust or has been purchased by another organisation such as the university or a company but is used and controlled exclusively by the Trust.

4 Introduction

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances the public interest.

This policy sets out how the Trust will meet its obligations in relation to information governance and information security.

The legal framework and standards relevant to information governance includes:

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Common law on confidentiality
- ISO/IEC 17799:2005 Information Security Management
- The NHS Information Security Code of Practice
- The NHS Confidentiality Code of Practice
- The NHS Records Management Code of Practice
- Caldicott
- Information Quality Assurance (data quality)
- Payment by Results Code of Conduct

There are five key strands to information governance:

1. Proactive use of information in the organisation for patient care and service management as determined by law and statute.
2. Proactive use of information between the Trust, NHS organisations and partner organisations to support patient care as determined by law and statute.
3. Commitment to make non confidential information widely available in line with FOI.

4. Effective arrangements to ensure confidentiality, security and quality of personal and sensitive information.
5. Information held is of highest quality in terms of accuracy, timeliness and relevance.

5 Responsibilities

Information governance and information security is the responsibility of everyone in the Trust. This section describes the specific responsibilities of certain individuals, as well as those of managers and individual members of staff.

Board responsibility: the medical director is the named executive director with responsibility for information governance.

Information governance steering group (IGSG): overall responsibility for overseeing the implementation of the information governance strategy, the information governance policy and information governance action plan.

Senior information risk owner (SIRO): A board level role to:

- lead and foster a culture that values and protects and uses information for the success of the organisation and benefit of its patients
- own the organisation's overall information risk policy and information risk assessment process, test its outcome and ensure it is used
- advise the accounting officer on the information risks aspects of the statement of internal control. Ensure board are aware of risks
- own the organisation's information incident management framework
- ensure that serious untoward incidents and data losses are reported in the organisation's annual report

Chief medical information officer/ chief information officer: our senior leaders within the Trust, accountable and responsible for the Trust's eHospital programme including:

- continued stabilisation of the eHospital programme
- development of longer term optimisation plan
- management of the Trust's technical infrastructure
- building on strong clinical engagement within technology transformation

Information governance lead: this role is responsible and accountable for managing information governance across the entire Trust at all levels, bringing together information governance management, confidentiality and data protection assurance, Caldicott compliance, information security assurance, cyber security, clinical information assurance, secondary uses assurance, freedom of information and corporate information assurance.

Is the Trust's named data protection officer, Caldicott officer, registration authority manager, privacy officer and Epic security co-ordinator.

Is responsible for the management of the information governance annual work programme and delivery of annual improvements against the national information governance toolkit standards.

The key objective is to continue to embed and implement the Trust's information governance strategy and to raise awareness of information governance with Trust staff so they understand its benefits, enabling them to use it as part of their day to day working practices and improve patient care.

Information security manager: responsible for providing information security advice and direction, monitoring and reporting on the state of information security within the organisation, deputising for the information governance lead and assisting the information governance lead with the information governance work programme.

Information governance team: responsible for undertaking tasks as directed by the information governance lead, supporting the information governance work programme.

Information governance owners (IGO): nominated senior managers with an area of expertise who are responsible for ensuring compliance with elements of the information governance toolkit, meeting level 2 standards and achieving or working towards meeting level 3 standards.

Caldicott Guardian: a senior clinician appointed by the Trust to advise on issues of patient confidentiality, in accordance with the Caldicott Principles. Oversees data-sharing agreements between the Trust and non-NHS agencies and may arbitrate on confidentiality issues not clearly defined in law.

Information asset owner (IAO): a senior person within a division or department who is accountable for a particular asset or group of assets. Specifically, this individual will:

- be required to complete the relevant CFH modules in the information governance e-learning training tool
- be supported by the information governance lead and IT governance lead
- undertake a strategic role and provide assurance to the SIRO that:
    - assets are managed efficiently: access rights are being appropriately managed, business continuity and recovery plans are in place for business critical assets, assets are available and that the confidentiality and integrity of each asset is protected
    - dependencies on other assets are managed and the nature of these dependencies is understood and accounted for

- an information asset register entry is maintained
- a risk assessment has been undertaken and any medium and high risks have an agreed action plan and that the requirements of the action plan are implemented in order to reduce the risk
- staff are aware of and adhere to the information governance policies and procedures, supporting a culture that values, protects and uses information for the success of the organisation and the benefit of its patients

Information asset administrator (IAA): this is a practical role covering the ongoing maintenance of the data held in the information asset register. Specifically, this individual will:

- provide support to the IAO
- be required to complete the relevant CFH modules in the information governance e-learning training tool
- for each asset under their control, the IAA will:
  - ensure that information governance policies and procedures are followed
  - recognise potential or actual security incidents
  - ensure that information assets are entered into the register and that they are accurate and maintained up-to-date
  - prepare risk assessment action plans for the IAO to approve (in consultation with risk officer and IG team as appropriate)
  - oversee implementation of risk assessment action plans in order to reduce risk to the business

Managers: to ensure that all staff comply with the policies and procedures and that they attend the Trust's mandatory training. To implement any necessary/ reasonable changes that are highlighted by audits. Ensure all staff sign compliance with the information governance code of conduct. To ensure that access to systems should always be according to job need and not status. Access levels should be sufficient for job need and no more and that system administrators are informed immediately about staff changes affecting computer use.

Information governance representatives: each department has a nominated information governance representative, and along with the department senior manager they are responsible for ensuring that staff comply with the relevant policies and procedures and undertake key tasks as directed by the information governance team.

All Trust staff: must adhere to the confidentiality clause in their contract, attend information governance training on a yearly basis, report any breaches of confidentiality and comply with this policy.

Head of information technology strategy: with overall organisational responsibility for IT service delivery, the head of information technology will ensure that:

- development of new systems is undertaken according to published standards and in line with the information security policy
- development and operational systems are separated where possible and change control and acceptance procedures are in place
- new systems are not purchased or installed and services commissioned without appropriate information security checks

General information governance

6 New systems, outsourcing of Trust service or joint venture between the Trust and a third party

The implementation of a new system, outsourcing of Trust service or joint venture between the Trust and a third party must comply with information governance requirements. All will require information governance approval prior to deployment.

Information governance compliance is required to:

- identify and manage risks
- avoid unnecessary costs
- avoid inadequate solutions
- avoid loss of trust and reputation
- ensure all contracts contain appropriate clauses
- ensure that all data processors working for the Trust comply with information governance requirements
- meet legal and information governance requirements

6.1 Master application list – new applications/systems or upgrades

No new or upgrade to an application/ system must be installed on the Trust network unless it has been approved to be added to the master application list by the CUH change board.

Please refer to the standard ‘master application list’ document for more information. Further information is also available on Connect.

Once reviewed by the CUH change board, the information governance team will advise the department if further document is required to ensure that the application/ system complies with information governance requirements.

This may include but is not limited to:

- completion of the IG checklist for software
- completion of a privacy impact assessment
- review of the contract
- completion of a system security template
- completion of the third party checklist by the contractor

6.2 Outsourcing of a Trust service or joint venture between the Trust and a third party

Departments should complete the IG checklist for contractors and forward this to infogov@addenbrookes.nhs.uk for review. This form is available on Connect.

This may include but is not limited to:

- completion of a privacy impact assessment
- review of the contract
- completion of the third party checklist by the contractor

6.3 Privacy impact assessment

Where appropriate, subject to certain conditions, a privacy impact assessment will be required for new applications/ systems or contracts. The information governance team will advise if a privacy impact assessment is required.

Please refer to the standard 'privacy impact assessments' document for more information. Further information is also available on Connect.

7 Information governance code of conduct

All new starters to the Trust will receive the information governance code of conduct in their staff handbooks. The code is a summary of the various information governance policies. All staff will be required to sign compliance with the information governance code of conduct and a record of this will be recorded on OLM.

For further information please refer to Connect and the induction checklist.

8 Training and awareness

All new starters will receive information governance training as part of their Trust induction and orientation program.

All Trust staff will receive an information governance yearly update.

Staff will be kept up to date on information governance issues.

9 Management of the information governance toolkit

All IGOs will be required to produce an action plan for the elements that they are responsible for to demonstrate how the Trust will meet the requirements of the information governance toolkit. These action plans will be monitored through the IGSG.

The IGO will be responsible for collating a list of evidence that is being used to demonstrate compliance with the information governance toolkit requirements.

The Trust's assessment of its compliance with the information governance toolkit will be submitted to Health and Social Information Centre as required.

The Trust will undertake internal and external audit as directed by the medical director.

Information governance will be reported quarterly to the eHospital operational programme board, which is a designated sub committee of the board.

The information governance quarterly report will monitor performance against key standards; the report will be presented to the IGSG.

10 Information risk assessment

Information risk is inherent in all administrative and business activities and everyone working for and on behalf of the Trust continuously manages information risk. The aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved. It is an essential element of information governance.

Please refer to the information risk assessment policy for further guidance.

11 Information governance audit program

The information governance team will regularly undertake audits to ensure compliance with information governance requirements. Reports will be available from these audits and action plans produced where necessary to ensure that any findings from the audits are implemented.

12 Audit of access to confidential information

Incidents are monitored by the information governance lead and IT governance lead. For further information please refer to the information governance incident and investigation procedure.

Audits are undertaken into access to Epic, as outlined in the audit access to patient records in Epic policy and procedure.

Privacy alert audits are undertaken by the information governance lead into staff accessing the system one clinical record viewer.

Break the glass alerts will be undertaken by the information governance lead as required.

IT service helpdesk and support team will inform the information governance team of any calls that involve misuse or sharing of passwords. The information governance team will investigate these incidents. If a member of staff is logged out of the system because a password has been shared, the IT service helpdesk will not reset the password until one of the information governance team has spoken to the member of staff.

A review will be undertaken by the information governance team on a yearly basis of all main applications/ systems that handle personal identifiable information to ensure they comply with the appropriate mechanisms that have been put in place to manage and safeguard confidentiality including a review of access rights, profiles, reporting, audit trails and to review a sample of forms requesting access to the system.

Medical records follow authorised access to the library, for further information please refer to the confidentiality of personal health information policy.

A summary of the findings will be included in the information governance yearly audit report provided for the information governance steering group.

13 Business continuity

Business continuity plans help organisations predict, assess and counteract threats and risks that may lead to events that seriously disrupt or curtail all or part of their business functions. The assessments analyse the probability of the events occurring, their likely impact and determine the procedures that the Trust should follow if such an event where to occur.

For further information please refer to the business continuity (BC) planning policy.

14 Policy exception

There may be exceptional circumstances where Trust staff require approval for a process/ device that will not fully comply with the Trust information governance policies, a policy exception form should be completed and submitted to information governance for a decision to be made as to whether the exception can be approved.

- If approved an exception will be either a temporary or permanent approval.
- Temporary approvals will be reviewed on a regular basis, as a minimum at least yearly.
- A permanent approval will result in an amendment to the Trust existing policy.
- A log of all requests is kept.

15 Breaches and incidents

It is each member of staff's responsibility to comply with the relevant policies and procedures that meet the requirements of information governance. Failure to comply with the Trust's policies, breach confidentiality or breach the Data Protection Act could result in staff being taken through disciplinary procedures which could result in the loss of employment.

Further guidance is available in the information governance incident and investigation procedure.

16 Protecting personal information

It is vital to keep information secure to protect the confidentiality and privacy of personal information. Photocopied or copies of information should be treated as originals and governed by the same Trust rules. The following measures should be adhered to at all times in relation to patient, staff, other personal information and confidential business information:

- supervise visitors in areas where personal identifiable data is held
- do not share security door codes with unauthorised persons
- do not leave information lying around on photocopiers for the next person to see
- prevent casual observation
- do not leave personal identifiable data lying around
- lock offices and clinical areas when unoccupied
- keep a log of key holders
- locate medical records storage trolleys in a location where staff can see them at all times
- lock away documents that contain confidential data and PID
- handovers must take place in private, unless they have to take place by the bedside
- try to maintain as clear a desk policy as possible

- think about where you are before you discuss confidential information
- screen prints must not be taken of any PC screen unless for a specific business purpose and only shared with colleagues where there is a legitimate reason for sharing the information

16.1 Transporting personal identifiable information

These processes must be followed when transporting PID:

- transport medical records face down in trolleys
- locked trolleys should be used where possible
- do not leave trolleys unattended in corridors
- always carry loose papers that contain PID securely. PID must not be visible to others during transport
- patients' notes must be placed in a sealed envelope when they are sent to appointments in other areas of the hospital

16.2 Taking PID off the hospital site

These processes must be followed when taking PID off site:

- PID should only be taken off site when it is required for the purpose of staff role
- medical records or copies of the medical records must not be taken off site unless for outreach clinics or for Coroners/ legal cases; this includes the residences on the Trust site
- when a member of staff leaves the Trust no PID must be copied and taken with them. Other Trust information may only be copied once approval has been obtained from the departmental manager
- any paper documents that contain PID must be transported in a locked bag
- medical records must be carried in a locked bag or box or transported by Trust approved courier
- information must not be left unattended whilst off site
- where possible, information must be returned to the hospital site on the same day. If this is not possible information must be kept secure in your home overnight
- mobile devices must be encrypted, please refer to section 6

16.3 Ensure patients are handed the right information

Care should be taken to ensure that patients are only sent or handed their own information:

- use windowed envelopes wherever possible
- don't use scrap paper in printers or photocopiers
- double check that the right information is being handed to the right patient

16.4 Handover sheets

These processes must be followed by all clinical staff including doctors, nurses, therapists and other healthcare professionals when using handover sheets.

16.4.1 Usage

- It is the responsibility of every member of staff to write their name at the top of each page of their handover sheet at the beginning of the shift.
- Individuals are responsible for the secure usage of handover sheets during the shift and the safe disposal at the end of the shift.
- All handover sheets should only contain essential information required for patient care and should be kept as brief as possible.
- Any handover sheet found in a ward area without a name should be handed to the nurse in charge for secure disposal.
- Handover sheets should only be printed at the beginning of each shift and allocated to named individuals.
- Any excess handover sheets should be securely disposed of by the nurse in charge.
- Electronic copies of handover sheets must be only saved on a secure network drive. They must not be stored on data sticks or desktops.
- Any handover sheet found either on or off the hospital site by a member of staff, or handed to a member of staff by a patient or member of the public, should be handed in immediately to the information governance team on (extension 256141/ bleep 154 247).
- If nursing staff are moved between wards during a shift the original handover sheet should be securely disposed of and a new one issued for the next ward.
- Handover sheets should not be taken off-site. The only exception to this rule is that doctors on call from home may take the relevant handover sheet off site for that on call shift. The policy which applies to taking confidential patient information off site is applicable to a handover sheet being used to support an on-call doctor.

16.4.2 Disposal

- Handover sheets should be disposed of securely in the confidential waste paper bins provided on wards and in all clinical areas.
- In addition there are confidential waste paper bins provided at every entrance and exit to the hospital buildings.
- If handover sheets are taken home to support on call, they must be disposed of securely in the home with the use of a cross-paper shredder, or brought back to the hospital at the first opportunity to be disposed of in a hospital confidential waste paper bin.
- Handover sheets must never be put into an ordinary waste paper bin, either in the hospital or at home, or into any other waste disposal bin other than one specifically designated for confidential paper waste. They must never be put into a domestic paper recycling system.

16.4.3 Handover sheet templates and good practice guidance

- Handover sheets should clearly be marked as such and have a designated space on the top right hand corner where an individual member of staff can write their name clearly.
- Handover sheets should have the ward name and date clearly marked on each sheet.
- Handover sheets should only contain essential information required for patient care.
- Use the Stop/ Check/ Bin logo where possible.
- Use the warning triangle and Information Commissioner fine potential where possible.
- Good practice is to minimise the use of ‘copy and paste’ to transcribe information from shift-to-shift to make sure that all information is relevant and accurate.
- New patient information should always be created on a fresh line/ cell/ row in a spreadsheet or table.
- The ward sister/ nurse in charge should make sure that there is a local ward policy for the usage and disposal of handover sheets and is responsible for ensuring that this process is followed on their ward.
- Spot checks may be carried out at any time by ward sisters/ nurses in charge or other Trust employee designated to do so from time to time.

16.5 Moving departments/ offices

These processes must be followed when staff move location or office:

- PID must be kept secure in transit.

- If a department is locating to another location temporarily, all PID must be moved to the new location.
- If any confidential information is no longer required then it must be disposed of securely.

16.6 Paper health records

Ensure notes are always placed faced down or covered by a blank sheet/ card, if placed in a wall mounted container place the notes facing the wall.

Where possible use a container to place notes in or keep notes out of view of the patients/ members of the public.

16.7 White boards and plasma screens on the wards

White boards and plasma screens are an invaluable tool for the wards to identify quickly where patients are located.

White boards and plasma screens should wherever possible be placed in locations away from public view.

Patients will be advised that we do display their names on white boards and plasma screens through the normal communication channels that advise them how we use their information.

16.8 Use of social media applications for the purpose of communicating with staff

Users who wish to set up the use of communication apps to enable easy communication in justifiable business circumstances must adhere to the following policy statements:

- Departments must register the use of communication apps with the resilience manager and information governance, using the designated information governance approval form.
- Each group must have a designated owner. You may assign a number of administrators as required to control new access and deletion of access, however the number of administrators must be limited.
- PID must not be shared via communication apps.
- No photos, videos or PID must be stored on the user's personal phone whilst using communication apps.
- When sending messages via the communication app users must check the recipients before sending messages to ensure all contact details are correct.

- Users are responsible for taking all reasonable steps to safeguard their device in line with the information governance and information security policy.
- Users must not screen print or copy the screen.
- Users must not voice record without acknowledgement and consent of those they are recording.

17 Safe haven procedures

Safe haven is a safe and secure process to receive and send PID. Wherever possible anonymise data before transmission.

17.1 Fax procedures

These processes must be followed when sending PID by fax:

- any confidential information held by the organisation should only be sent by fax where it is absolutely necessary, justify why you are faxing the information
- patient identifiable information should only be sent by fax, in an emergency situation, where possible send from an NHS Mail to NHS Mail email address as this is free
- ensure that fax machines are located in secure areas at both ends of the transmission
- always double check the fax number to which you are sending information
- if you are unsure about the number you are sending a fax to, do not send the information without verifying the number with the recipient
- use pre-programmed numbers where possible to avoid misdialling
- contact the recipient before sending to let them know you will be sending a fax
- ask the recipient to acknowledge receiving the fax immediately
- confidential faxes must not be left lying around for unauthorised staff to see
- don’t allow faxed information to remain uncollected on the fax
- make sure the fax cover sheet is marked private and confidential and states who the information is for
- use NHS choices to search for NHS fax numbers, don’t use Google etc

Fax machines should display the safe haven fax poster near them; these can be obtained from the IG team.

The Trust has a designated safe haven fax machine, which is located in the general office in the medical records corridor on Level 3. The fax number is 01223 414771. The office is always manned during working hours and locked at night. The fax machine is only used by a limited number of people and there is no access to members of the public.

17.2 Surface mail (post)

These processes must be followed when sending PID by post:

- correspondence must be sent in a sealed envelope and to a named individual
- if sending very sensitive information also mark the envelope private and confidential
- open incoming post away from public areas
- if sending sensitive information to a third party, consider using special delivery or Trust approved courier as appropriate
- the use of windowed envelopes for patient correspondence is allowed as long as only the name and address of the addressee is visible in the window, no other details should be visible such as “dear Dr”, hospital number or Trust logo, the letter must be folded tightly in the envelope so as to avoid any movement; undertake the shake test

17.3 Telephone

These processes must be followed when contacting patients by phone

- telephone calls relating to patients/ staff should take place in private
- record and replay answer machine messages/ voice mail in private, use headphones if confidentiality cannot be maintained

When contacting patients, if you get an answer machine or another member of the household picks up the phone:

- only disclose the specialty clinic that you are phoning from if you have the consent from the patient

If you do not have patient consent:

- If the call is not urgent find out when the patient will be at home and call back; do not provide any contact details
- If the call is urgent leave your name, contact number and that you are phoning from Addenbrooke’s/ Rosie hospital; do not disclose any other clinical details; ask for the patient to contact you when they are home

17.4 Emailing patient identifiable information

Emailing PID is not secure and should only be sent in accordance with this policy. NHS Mail (nhs.net) was created especially for the exchange of sensitive information between NHS organisations.

Only include the NHS number or medical records number (MRN) in the subject heading, never include any other PID details.

Do not email information to your home email account; use an NHS Mail email account which is accessible from all PCs via the web.

When contacting other NHS organisations, only send email from and to an NHS Mail email account. Further information on NHS Mail is available on Connect.

When contacting colleagues within Addenbrooke's, only send emails from and to an Addenbrooke's email address or from and to an NHS mail account. Never use any other email addresses.

When contacting other external non NHS organisations, either anonymise the PID within the email, encrypt the attachment using windows 7 zip to encrypt the file (see 7 Zip instructions) or use NHS Mail secure service for non NHS mail; further details are on Connect.

Certain organisations have an agreement with the NHS to use NHS Mail, and hence secure communications is possible with them. (See HSCIC Secure email Page).

17.5 Communicating with patients via email

- Before sharing any information via email patient consent is required.
- Only share appropriate clinical information by email with patients.
- Verbal consent can be accepted from the patient, patients must be made aware as part of the conversation that email is not a secure method of communication, the wording in the paragraph below can be used to form part of the conversation, the patient must accept the risk of using email before you can communicate with them by this method.
- If an email is received from the patient, the paragraph below should be sent to the patient by email to outline the risks of using email, the patient must accept the risk of using email before you can communicate with them by this method.
- Record their email address on Epic.
- Document the consent whether verbal or by email in a note in Epic.

17.5.1 Risk statement for patients on the use of email

"The use of email is not a secure method of communication, emails can either be intercepted during transit, sent to the wrong address by the sender or receiver or viewed by other members of the household.
The Trust will ensure that it puts in place safeguards to ensure that any communication by email is appropriate and that we check your email address against that recorded on your record before sending the email.
We ask that you notify us immediately if your email address changes or you no longer wish to receive communication by email.
Please confirm by return of email/verbally that you are happy to proceed with the use of email as a method of communicating with the Trust."

17.6 Emailing staff information

Staff names should not be included in the subject heading of emails. When sending very sensitive information by email follow the same rules as patient information.

17.7 Emailing confidential business information

When sending confidential business information by email follow the same rules as patient information.

17.8 Request for information from external agencies

If you receive a request for information over the telephone ask for the request to be confirmed in writing by fax on headed paper. If they are unable to send a fax, take their switchboard number, name and extension number and phone back through the switchboard. Do not use direct line numbers as it is not possible to check the identity of the caller.

17.9 Bulk transfers of personal information

A bulk transfer is defined as the sharing of information that includes personal identifiable data for 51 or more individuals' details in one request.

A log of bulk transfers will be held by the information governance team; inform the information governance team if a request for information will include 51 or more individuals' details.

Applications and services

18 Information asset register

As part of the information governance toolkit, the Trust is required to build and maintain a register of all its major information assets:

- each asset is assigned an IAO
- each asset must be assessed for its criticality
- all critical assets tier 1-3 and those holding PID must have risk assessments in place covering unavailability and breach of confidentiality
- all databases and applications that hold PID must have a documented system security template (SST) (see system-level security policy)

For further guidance please refer to the information asset user guide.

19 Email

All CUH staff will be automatically issued with a CUH email address by default which is considered to be their primary email.

Access to an NHS mail account will be used as an alternative to a CUH email if a business needs arises.

Where staff have multiple email accounts they should ensure that the CUH email account is checked on a daily basis.

19.1 Acceptable use

Occasional personal use of the Trust email system is permitted for personal use outside of the employee's working hours.

Any personal emails must explicitly state that the communication is being sent in a personal capacity.

Staff may use their work email address for personal communications but these emails must be dealt with outside of working hours.

The use of the Trust email service for private commercial purposes or the unauthorised advertising of goods and services is strictly forbidden.

Any emails sent must not contain any offensive or inappropriate material.

The use of the Trust email service outside of the above could lead to disciplinary action being taken against the staff member. In some circumstances misuse may be considered as gross misconduct and could result in dismissal.

19.2 Mailbox sizes

Staff are expected to maintain their email in line with retention schedules and within their allocated storage space.

The allocated mailbox size is per email account and including inbox and sub folders, sent items, deleted items, tasks, calendar and contacts.

If users receive a large volume of emails that regularly exceeds the storage allocation then additional storage space can be requested and will be provided subject to budget holder authorisation.

19.3 Management of email accounts

Emails are not private property and remain the property of the Trust.

Email should be seen as a transitory storage. Emails that need to be retained must be saved in your allocated network folder area according to the guidance in the Trust retention and destruction schedule available on Connect.

Each member of staff is responsible for managing their email folder within their allotted storage allocation, guidance on how to manage emails is available on Connect.

Automatic forward of emails is only allowed to internal CUH email addresses.

19.4 Email format

All Trust staff must comply with the Trust standards for format as outlined in the corporate identity styles available on Connect.

All Trust staff must comply with the Trust standards for signature as outlined in the corporate identity styles available on Connect.

All Trust staff must use the Trust standard disclaimer as outlined in the corporate identity styles available on Connect, the standard disclaimer should be included as part of the signature.

All Trust staff must include an out of office message when they are away from the Trust using the standard out of office message as outlined in the corporate identity styles available on Connect. An out of office reply will only be sent once to a recipient during a period of absence. Out of office messages will be sent internally and externally.

19.5 Email addresses on the global address list

Only CUH or NHS Mail email addresses will be entered into the global address list. In exceptional circumstances non standard email addresses may be added

to the global address list, to apply please refer to the information governance operational manual.

19.6 Email filtering

All external incoming and outgoing emails must pass through an email filtering system and will be scanned automatically for spam, viruses and other unacceptable content, no email content is visible to HP.

Staff must not forward any emails that display warnings about viruses or other computer security issues that they may receive to any other staff, staff should contact the IT service desk.

If Internet gateway antivirus software detects a virus the email will be rejected, there will be no message to the sender or recipient.

Some email addresses such as web based email are blocked at the perimeter of the network. In exceptional circumstances blocked email addresses will be allowed, such as doctors.net.uk, but to request the unblocking of an email address please refer to the information governance policy exception process in the information governance operational manual.

Some attachment types are blocked as these are frequently used by viruses, a list of blocked file types is available on request.

19.7 Distribution lists

Distribution lists can be set up using entries in the global address list for internal use. Each distribution list must have an owner who is responsible for maintaining the list.

If the owner of the distribution list leaves the Trust they are responsible for ensuring that a new owner is identified and that the service desk is informed of the change.

19.8 Generic email/ calendar account

The Trust allows generic email/ calendar accounts to be set up to simplify work processes allowing a number of staff access to the account as appropriate.

Each generic account must have an owner.

If the owner of the generic account leaves the Trust they are responsible for ensuring that a new owner is identified and that IT are informed of the change.

To apply for a generic account please refer to the information governance operational manual.

19.9 Email recovery

In exceptional circumstances email can be recovered. Requests should be raised via through the IT service desk and then approved by information governance if necessary. Please refer to the information governance operational manual.

19.10 Access to and monitoring of email accounts

The Trust reserves the right to inspect any emails stored in the network and or PCs. Access would only be granted where there is a clear and justified requirement or suspicion of breach of Trust policy and will be agreed with human resources.

Emails marked 'private' will only be accessed if there was a justified business need or the Trust was investigating an incident.

In exceptional circumstances, where there is a legal dispute or tribunal, a mailbox can be placed under legal hold; this would only be activated on the authorisation of human resources, information governance or medical legal. Please refer to the information governance operational manual.

If an employee is absent in unforeseen circumstances it may be necessary for the Trust to access their email to ensure the continued provision of services. Managers must follow the temporary account access process outlined in the information governance operational manual.

Emails may have to be disclosed to outside sources under the Data Protection Act or Freedom of Information Act.

Audit logs are available for mailbox activity, audit logs would only be requested where there is a clear and justified requirement or suspicion of a breach of Trust policy and will be agreed with human resources.

A multi mailbox search for information discovery purposes is available and would only be used where there is a clear and justified requirement, for eg receipt of a subject access request, and will be agreed with human resources, medical legal or information governance. Please refer to the information governance operational manual.

20 Internet

As a wide variety of materials may be deemed offensive (by colleagues, patients, the public, or suppliers), the display of any kind of sexually explicit image or document or any other material on any Trust system which would breach the Trust's equality, diversity and inclusion in employment or grievance and dignity at work policies is unacceptable. Such behaviour may be considered

as gross misconduct under the Trust's disciplinary procedure and could result in dismissal. In addition, such material may not be:

- archived,
- stored,
- distributed,
- edited, or
- recorded

using the Trust's network or computing resources. This applies regardless of which Trust system is used and whether this behaviour takes place out of work time.

Internet access is for business and limited personal use -- unauthorised personal use of the Internet during working time could be considered fraudulent behaviour and may result in disciplinary action in line with the Trust's disciplinary procedure and could result in dismissal.

Access to websites is managed by software that categorises access and restricts access. Request for blocked user categorisation will be managed through information governance approval. Access to sites is monitored by IT.

Anonymous access to the Internet is not permitted.

Instant messaging and online chat tools may not be used on any Trust computers and will normally be blocked. If there is a legitimate business need to use these tools, then explicit permission from both the line manager and the IG must be obtained.

Only those employees or non-executive directors who are duly authorised to speak to the media or in public gatherings on behalf of the Trust may speak/ write in the name of the Trust to any forum. Other employees may only contribute in an electronic forum in the course of business when relevant to their duties with the explicit approval of their heads of department.

Any employee using the Internet facilities of the Trust shall identify himself or herself honestly, accurately and completely when participating in forums as part of their duties, or when setting up accounts on outside computer systems.

The Trust retains the copyright to any original material posted to any forum by any employee in the course of his or her duties.

While employees may self-publish to a forum in their own time and using non-Trust computer equipment, the following rules **must** be followed:

- It must be very clear that views are strictly those of the employee.
- You must not mention that you work for the Trust.
- Do not discuss or get involved in discussions concerning the Trust, patients or other staff.

- Do not reveal any confidential information, any patient, Trust or employee data, research material nor any other material covered by existing Trust confidentiality policies and procedures and/or Code of Business Conduct.
- If discussing controversial issues or those related to healthcare or the NHS, care must be taken not to use examples that could identify the Trust or patients.
- You should not display images of Trust property or premises unless they could reasonably have been taken by any member of the public.

Employees breaking these rules, whether or not the breach is inadvertent, may be subject to disciplinary action under the Trust's disciplinary procedure, and this could result in dismissal.

Individual employees as well as the Trust are potentially liable to be sued for defamation. Posting to Internet forums as well as email, even inside the Trust, are forms of publication. Defamation is either libel or slander, and is described as comments which lead to the lowering of someone in the views of others. Trust Internet facilities or email must not be used for potentially libellous or slanderous purposes.

20.1 Security

Any file that is uploaded or downloaded must be scanned for viruses before it is run or accessed. If a member of staff is unsure of whether their system has a virus checker installed they should contact the IT service desk.

The Trust has installed various systems to assure the safety and security of the Trust's networks. Additional devices and software may also be installed in the future to further protect these networks. Any employee who attempts to disable, defeat or circumvent any Trust security facility may be subject to disciplinary action.

No employee may use the Trust's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Connections to the Internet using modems from network connected computers are specifically prohibited.

21 Wi-fi

The Trust currently has a corporate wi-fi infrastructure which should preferentially be used for the delivery of any requirement for services based on wi-fi. Alternative wi-fi arrangements should only be put in place if the corporate infrastructure cannot fulfil the need, and in this event, approval must be sought through information governance and information security.

Access to corporate wi-fi services should be linked to a domain user name, and be managed through a user registration process.

In order to optimise bandwidth utilisation, corporate wi-fi services should only be used for business purposes.

22 Printing and scanning

22.1 Printing

Networked printing services are provided throughout the Trust. Local printers will continue to be available for thermal, Meditech and HISS printing until no longer needed.

Staff must ensure that they collect all printed material from the printer. Information must be carried securely around the hospital site.

Fobs will be issued to all staff to enable printing and will be attached to ID badges. Fobs will be issued to new staff via the access office. A fob is linked to the member of staff and should be treated with the same security awareness as a password so should not be handed over to another member of staff to collect printing on their behalf. However delegate printing is available for staff who need someone else to collect their printing on behalf of them.

If a member of staff losses their fob then this must be reported to their manager and IT service desk as soon as possible so that the fob can be deactivated and a replacement organised. Replacements will be available from the access office for a small replacement fee.

22.2 Scanning

This section does not apply to the scanning of medical records.

Scanning to self is available from the managed print service devices, by default scanned documents are sent to your CUH email account. Flatbed scanners can also be used for scanning to a department document storage area.

Scanning to a department document storage area can also be set up from the photocopier devices subject to information governance approval; staff must submit an information governance approval form for approval.

Any requests for scanning to email addresses other than your own should be made through information governance.

23 Remote access

- Should only be permitted through approved remote access solutions.
- Two factor authentication is required for any solution accessing patient identifiable information.
- Should only be provided for those with a business need.
- Should be removed from those who leave the Trust.
- Records must be kept by the information asset owner of all accounts and the level of access provided, these must be maintained and current and available for audit on request.
- Remote access logs must record changes to access, new access, deletion of access, successful login date & time and failed logins.
- All access must be limited to an appropriate level determined by the member of staff's role.
- All access must be reviewed on an annual basis; an audit trail must be kept of this review.
- All user accounts must be associated with a named individual.

24 BYOD

The BYOD policy applies to any Trust-owned or privately owned device which uses the BYOD framework to access Trust data and services. For use of any device outside of the BYOD container, please refer to the mobile device policy section.

The user agrees to the Trust having complete and ongoing control over the BYOD container on their device (using a third party mobile device management solution) – the Trust is able to update applications or install updates as required.

The Trust will only support the BYOD service on personal devices. Trust purchased iPads will be supported by central IT.

Connection to the BYOD container will be via any Internet connection, internal CUH wireless or mobile provider network connectivity.

All data in transit between the Trust network and the device is encrypted to NHS security standards. Any Trust data located on the device during a BYOD session or persistent thereafter will be automatically encrypted to NHS standards inside the BYOD container.

Applications available through BYOD should only be able to print to corporate printers, with no capability to print to devices connected locally to the device by whatever means. Copying or movement of data is not allowed from the BYOD container to the device.

Any application which is designed to give access to Trust data on a mobile device should be approved by IG, packaged and delivered securely through the BYOD service.

Devices must be set to automatically lock after five minutes of inactivity. Once the device is unlocked, access to the BYOD container will be via single factor authentication.

Security settings on the device and for each application will be set as per the CUH BYOD policy table. Settings will vary for Trust devices and personally owned devices.

Where a BYOD-enabled device has been lost or mislaid, it should be reported to the service desk within 24 hours so that it can be remotely locked for security purposes. Where a BYOD-enabled device is known to have been stolen, the theft should immediately be reported to the service desk who will lock the device remotely and wipe (reset) the BYOD container for security purposes. The owner of a private BYOD-enabled device which has been lost or stolen may request that the device be completely wiped, but this is strictly at the owner's risk.

The device will be automatically lock after 10 failed login attempts. Staff should contact the service desk for the device to be unlocked.

When a member of staff leaves the Trust the BYOD container will be remotely wiped.

Access to Trust email must remain separate from private email at all times. Automatic forward of emails is not possible between Trust email and private email account.

Personally installed apps cannot access any of the data in the secure container.

Only devices that meet with the Trust standards will be allowed to connect to the Trust's BYOD solution. Information on the standard devices that are supported by the BYOD solution are available on the Trust's intranet.

For timeout periods please refer to the 'time out policy' section within this policy.

On no account should any personal identifiable information regarding Trust staff or patients be stored or processed on the device outside of the secure container or on any cloud services to which a personal device might be connected.

Access to BYOD service will not be available to a device modified for root access, commonly referred to as 'jail breaking'.

25 Remote access to email

Users who wish to access Trust email through either web services or apps must adhere to the following policy:

- Users must set a password or PIN on their device.
- Care must be taken to avoid casual observation.
- Where possible email push notification must be disabled on a personal device during annual leave/ non-working hours.
- Automatic screen locks must be enabled on the device.
- Data must not be saved from email to a local PC or device.
- Any printing of documents must adhere to section 7 of this policy, 'taking information off site'.
- Devices that have been modified by 'jail breaking' should not be connected to remote access email services.
- It is important that sensitive/ personal identifiable data isn't held on a device that does not have encryption enabled.
- Staff must always log out/lock access when away from the device/ PC.

Users of remote access to email must be aware of:

- Remote access does not support shared mail boxes, if this access if required users will need to register for BYOD access.
- Users receiving data to their own device may incur a financial cost, depending on your contract.

26 Desktop standards

The Trust is rolling out a desktop standard that includes:

- Logon screen – security wording will be displayed.
- Splash screen – no image, plain.
- Desktop background – plain with no text/ graphics.
- Screen saver time out settings.
- Time out settings.
- Desktop short cuts – users should be able to create their own shortcuts as long as restrictions are in place on command utilities.
- Locked down start up menu.
- Control panel – restricted settings available only basis settings such as mouse or sound can be changed.

27 Web conferencing facilities

- Online meetings must not be recorded/ videoed, if recordings are required, approval must be sought from information governance.
- Screen sharing and or remote control has to be accepted via an on-screen prompt before the host can use this functionality.
- If sharing a PC screen with external organisations/ contractors ensure that no PID is visible unless the purpose of the meeting is to discuss the PID.
- Screen prints of your PC must not be taken by the external organisation/ contractor.
- Approval must be sought from information governance if you wish to upload documents to the meeting site.
- Documents must not be uploaded if they contain PID.
- Documents must be held on the site securely.
- The only documents that can be uploaded must be relevant to the meeting.
- Documents must be deleted from the site in a timely manner.
- The use of web conferencing for patient discussions/ involvement must be approved by information governance.
- If a patient is participating in the web conference their consent must be sought first before taking part in the conference.
- Check that the right people have joined the meeting before commencing the meeting.

Access to data and systems

28 Visitors with visibility of or access to the Trust's information assets

In certain situations visitors to the site may require access to the Trust's information assets or have visibility of the confidential patient information because of the areas they are visiting, but not all of these visitors will have a contract agreement with the Trust. These visitors to the Trust must sign a confidentiality statement, a copy of which is available from information governance. Advice is available from the information governance team.

29 Request to share an extract of a database or copy of a database with a service provider contractor

Where there is a need to share personal identifiable data with a service provider contractor eg they require an extract of a database to fix a problem or they require data to perform an analysis on behalf of the Trust and that data cannot be anonymised, the third party contractor must firstly sign the data protection contractor form, which must be completed before any data is shared. This form is available as a word document on Connect. The contractor must copy this form onto their headed paper. A copy of the signed form must be sent to the information governance lead.

Once approval has been received from information governance to share the data with the third party contractor the database must be sent in a secure manner either by encryption or uploading to a secure site. Please contact the IT service desk for further advice.

30 Home working

Subject to line managers approval staff may work from home regularly or occasionally but staff in this position must continue to comply with all aspects of this policy and the policies listed in section 52.

- Where possible, access to PID/ business confidential must be through the Trust's remote access solutions; if this is not possible PID must be held at all times on an approved encrypted mobile device.
- Staff must not forward PID from their work's email address to their home email address.

Whilst working at home:

- avoid leaving mobile devices within sight of ground floor windows or within easy access of external doors
- do not leave PID/ business confidential information lying around
- hard copies of documents containing PID/ business confidential information must be destroyed at the Trust unless you have a cross-cut shredder
- data must not be transferred from a mobile device to your home PC
- all Trust data must be returned to the Trust for storage/ retention

31 Working off site

As part of their role staff may be required to work at another location in order to deliver NHS services, staff in this position must continue to comply with all aspects of this policy and the policies listed in section 52.

- Access to Trust electronic data will be via the Trust remote access solution.
- It is recommended that staff carry the minimum amount of information with them, especially during home visits.
- All Trust data must be held securely so that it is not accessible by non-Trust colleagues who work in the location where the member of staff is based.
- Printing documents off site is allowed where the functionality of the system that you are using allows this, any paper documents generated from printing must then be kept secure in compliance with this policy.
- Do not leave PID/ business confidential information lying around.
- Hard copies of documents containing PID/ business confidential information must be destroyed at the Trust unless you have a cross-cut shredder.
- All Trust data must be returned to the Trust for storage/ retention.

32 End point control

All PCs connected to the Trust core operational network must have installed device control software unless a policy exception form has been approved by information governance.

End point protection software has been configured to control the use of mass storage devices such as USB memory sticks and external hard drives.

Staff will only have read only access for all mass storage devices connected to their Trust PC, read and write access will only be available for Trust approved standard devices or devices approved by information governance.

The Trust will maintain a compliance list of approved devices which will be reviewed on an annual basis.

If staff require read and write access to a non standard mass storage device they must complete a policy exception form and submit this to information governance for approval.

33 Access to systems

This is applicable to all system accounts including user accounts, service accounts, privileged user accounts and support accounts.

- All information systems must apply appropriate authentication controls in line with the sensitivity of the data held within or transmitted across them.

- Access to all applications must have a documented procedure that complies with this policy, please refer to the system level security policy.
- All system access requests, changes and deletions must be approved by an appropriate member of staff.
- Records must be kept by the information asset owner of all accounts and the level of access provided, these must be maintained and current and available for audit on request.
- No individual will be given access to a live information system unless properly trained and made aware of their security responsibilities.
- All access must be limited to an appropriate level determined by the member of staff role.
- All access must be reviewed on an annual basis, an audit trail must be kept of this review.
- No single member of staff should be able to authorise all access to a system.
- All user accounts must be associated with a named individual.
- All service accounts should have a nominated owner.

34 Access profiles

Access profiles must be documented and approved by an appropriate meeting/ manager; please refer to the system level security policy.

35 System logs

System logs must record changes to access, new access, deletion of access, date and time of login and failed logins.

36 Leavers and inactive accounts

- Leavers reports will be generated by HR, circulated to HP systems administration team and information governance on a weekly basis.
- Leavers who leave the Trust will have their access to all systems made inactive immediately.
- HP systems administration team will produce an inactive account report on a monthly basis, identifying any accounts that have been inactive over the last 90 days. This report will be reviewed by CUH to identify accounts that can be deleted.
- Domain accounts will be deactivated and hidden for 90 days and then permanently deleted; deletion will include exchange and home-drive personal storage space.

- Line managers can request access to a user's home-drive space during the 90 days to review the content before it is deleted.

37 Shared accounts

In order to simplify work process, there are sometimes requirements for generic or shared accounts. These can pose a significant security risk, allowing untraceable access to systems. For this reason login accounts with generic names and shared passwords must not normally be created in any system.

Shared or generic accounts must be agreed and approved by information governance by completing a policy exception form.

38 Password management

Applies to all application systems, domains, systems administration services and single sign on.

- All access to all information systems must be by unique ID and password (or other secure user authentication method approved by information governance).
- All users will be allocated a unique login ID.
- A default password may be used when the account is set up, but the user must then be prompted to change the password when they first log in.
- **Users must keep their passwords secret; passwords must not be written down**.
- **Users must not share their password**.
- **Accessing a computer system using another staff member's ID is strictly prohibited**.
- Where technically possible all application accounts should authenticate users against the domain account (active directory).
- Information systems must enforce the password policy, making it impossible for any user to select a weak password.
- System default accounts and passwords must be removed from all systems.
- When data is sent to another person in an encrypted format the password required to access that data must be shared by a separate form of communication.
- If any of the above conditions cannot be complied with then a policy exception form must be completed and submitted to information governance for approval.

- Users must not save any Trust passwords whether domain or for any software/ applications in Windows 10.

Passwords must be:

- a minimum of eight characters
- a mixture of upper and lower case letters and numbers
- set with a strong password (guidance for staff on the setting of passwords is available on the Trust's intranet)

Passwords can be set to non expire so long as all the conditions of this policy are complied with; approval to set a password as non expiry must be approved by information governance.

A password must be changed if staff suspect that their password has been compromised.

39 Password resets

- Ten failed attempts results in an automatic lockout.
- For service desk resets, DOB and name and an answer to one question set within the self service reset system is required.
- For self-service resets: the user can select six questions, three are used for resets and these can be changed by the user any time.

40 Data back up

All data should be considered for assessed to determine its back up requirement and appropriate technical measures employed to fulfil the requirement.

All data back ups should be protected appropriately.

Back ups should be undertaken in order that the Trust can comply with the data retention policy.

41 Data storage

No data should be stored on Trust systems unless it is directly connected with or in support of Trust activity.

Trust data must not be stored on the local PC. Note that the 'my document folder' is a networked folder.

All data/ applications/ databases must be stored on the Trust centralised storage provision, provided by our IT contractors. Data stored in either of these

environments is secure, backed up under a support contract, regularly patched and disaster recovery is in place.

Subject to a business justification, information governance and technical approval data could be stored on servers either in another data centre or hosted locally by an IT lead as long as:

- The data is held in a secure environment, backed up, regularly patched, under a support contract and disaster recovery is in place. Consideration could be given for relaxing the rules for archive data, requests would be considered on a request by request basis.

Use of portable storage devices will only be approved as a temporary solution, subject to information governance approval; eg transfer of data from one network to another or temporary storage until a longer term solution is in place.

42 Use of data sharing websites for the sharing of Trust documents with external organisations

Staff or departments may have a business justification for sharing Trust documents with external organisations and due to either the size of the file or content of the document the preferred option would be to use a data sharing site. This will only be allowed subject to compliance with the following policy statements:

- The documents must not contain patient identifiable data.
- Access to data sharing sites will only be allowed following approval from information governance.
- Access to data sharing sites will be restricted to users approved by information governance.
- Data sharing sites must not be used as a primary source for the data, their use must only be to serve the purpose of sharing documents across organisations.

Devices

43 Mobile devices

This section applies to all mobile devices that can be used to store, view or process Trust data.

Staff are responsible for:

- taking all reasonable steps to safeguard the device in line with published guidance

- ensuring that they take sensible and reasonable precautions to avoid the viewing of sensitive data by unauthorised individuals eg by over the shoulder viewing or similar lapses of security
- ensuring that where devices are shared by family members that family members are not able to access Trust data
- all contract costs for purchasing or using the device unless prior agreement has been obtained from their line manager to claim some of the costs back

Users must not screen print or copy the screen unless on request of service desk.

43.1 Applicable controls for mobile devices

- The Trust will publish a list of a standard devices.
- Mobile devices should be made available for audit as requested.
- Data on mobile devices must not be used as the primary source of information. If working off line information must be transferred to a Trust network folder as soon as possible and deleted.
- Users must ensure that data is not transferred from an encrypted mobile device to an unencrypted non Trust device.
- Users must take reasonable steps to physically secure mobile devices.
- Mobile devices must not be used for Trust business if the security of any device cannot be assured.
- Non standard mobile devices must be approved by the IGAF, please complete the portal request on the HP service portal.
- Mobile devices used in conjunction with medical devices to store or transfer data should be encrypted where possible. If not possible an information risk assessment must be undertaken to determine the appropriate control measures that should be in place.
- The use of a mobile/ smart phone in the Trust must comply with the mobile phones and other mobile communications equipment policy.

43.2 Register of mobile devices

The Trust is required to maintain a register of mobile devices. The mobile device register form must be completed or updated when:

- a new mobile device has been purchased
- a mobile device is to be decommissioned
- there is a change of user

Further guidance is available on Connect.

43.3 Trust owned devices

All Trust owned devices must be encrypted unless they are used solely as a mobile phone or to access the Trust remote access solution. Exceptions to this policy must be approved by information governance, Trust wide exception will be published in the Trust standard device list.

Trust owned devices must only be used to hold Trust Data. Staff must not store any personal information such as files, games, personal photographs; movies etc on the device but may store personal organisational data such as appointments or personal contact details.

Trust owned devices must be returned to the manager when staff leave the Trust. The device can then be reformatted or destroyed securely as appropriate.

43.4 Private devices

Private devices must only be used to access the Trust remote access solution or as a mobile phone. Exceptions to this policy must be approved by information governance. Trust wide exception will be published in the Trust standard device list.

43.5 NHS Mail – access via a smart phone

NHS Mail is accessible via a smart phone where the smart phone enables the data at rest on the device to be encrypted, where this functionality is not available on the smart phone then it must not be used for NHS Mail access. Further guidance is available at www.nhs.net.

44 Mobile phones

The use of mobile phones by patients, visitors and staff must comply with the mobile phones and other mobile communications equipment policy.

45 USB devices

The purchase of USBs must be approved by information governance; the purchase of USBs will only be permitted for certain functions.

A register of all USBs will be maintained by information governance.

46 Haiku and Canto – taking clinical images

Mobile phones and tablets that have access to Haiku and Canto (Epic remote access app) can be used to take clinical images of patients. Patient consent must be taken using the trust standard photography consent form. A photograph

of the consent form must be taken and uploaded to the patient record along with the clinical image.

47 Multi function devices

The hard drive of multi function devices, combined photocopiers, scanners and printers, must be encrypted and disposed of securely. Where a multi function device is used for network printing security controls must be in place to ensure documents remain confidential and secure.

48 IT equipment

48.1 Purchase of IT equipment

- The purchase of IT equipment must always be approved by the head of IT and follow the Trust's procurement policy.
- Only authorised devices should be connected to the Trust's network.
- All IT equipment used for Trust business must have a unique identifier (asset tag).
- Equipment not owned by the Trust must not be connected to the Trust network unless approved by IG prior to connection.
- No modifications to the local network must be made outside of managed change control.

48.2 System patching

End user equipment, servers and infrastructure components should have up-to-date operating system security patches installed to protect these assets from known vulnerabilities. The suitability of any patch should be assessed for applicability and risk, and be deployed via the change control process.

Patches, and any other changes to the hardware or software configurations of any system should only be carried out by authorised individuals or third parties, and such changes be supported by appropriate technical and/or governance paperwork.

Adherence should be maintained with the 'the standards for the patching of computer systems and applications'.

48.3 Physical

- IT equipment must be installed and sited in accordance with the manufacturer's specification.
- Multi-user computer equipment, LAN and WAN equipment and other information servers holding sensitive or important data must be sited in a

secure area, where only authorised entry will be permitted. This should normally be a designated computer room or cabinet, which has been physically secured, and has fire protection measures. Rooms should be clean and away from pipework wherever possible.

- Computer rooms should also have environmental controls to keep equipment cool with remote monitoring to ensure an alarm is triggered if problems occur.
- Computer equipment should be assessed for its continuity requirements (power, back ups etc) and adequate resilience provided.
- Computer equipment must where possible be positioned away from ground floor windows and not adjacent to doors or public areas, etc.
- Physical locks are not required for workplace 360 machines or laptops.
- The hard drive for the workstation on wheels (WOW) will be locked in the WOW trolley.

48.4 Off site

Trust computer equipment will not normally be permitted to be taken off site. Exceptions to this include mobile devices, designated equipment for senior managers or clinicians to enable work to be done at home, and equipment being sent away for repair.

Any equipment taken off site (including mobile devices) must not be used for any purpose other than for duties associated with the member of staff's role in the Trust.

48.5 Software

The Trust is committed to the legal use of software. It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action.

Only standard and approved software is to be installed on Trust PCs.

Where a department needs specific specialised PC products, such products should be approved by information governance and the design authority.

Downloaded add-ons, tool bars, screen saver programs, games etc **must not** be installed on any Trust PC. This type of software can affect the running of other software and may contain hidden malicious code which could compromise information security.

Up to date information of all proprietary software must be maintained as part of the Trust's information asset register by all departments to ensure that the Trust is aware of its assets and that license conditions are followed.

48.6 Virus protection

The Trust views viruses and other malicious software as presenting a significant threat to information systems, and it is a disciplinary offence to wilfully introduce a virus or other malicious software onto the Trust's computer systems.

All active electronic devices running an operating system that are attached directly or indirectly to the Trust network, and are capable of sending, receiving, or forwarding information over the network must run up-to-date antivirus software in line with the current Trust standard. Exceptions including third party computers or other devices that cannot host our standard must be approved by IT prior to connection and may require information risk assessments to be carried out if appropriate.

All files introduced to the Trust's systems must be scanned for malware using an up-to-date anti-malware solution.

48.7 System monitoring

In order to maintain and improve the Trust's compliance with legal and regulatory software and data security requirements, the Trust will as necessary audit and monitor all deployed electronic equipment for hardware and software configurations, data movements between devices and the connection of any device to either the Trust network or to Trust computers. Based on this monitoring, steps will be taken to improve the Trust's compliance situation where needed and to address non-compliance of any type through whatever cause.

49 Time out

- All users who do not share a PC should lock their PC when they walk away from their desk using Ctrl-Alt-Delete.
- All users who share a PC should log out of any applications when not in use.

By location of device
The Trust PC will lock after periods of 30 minutes of inactivity

Third parties

50 Third party contractors

- All contracts must contain appropriate information governance clauses.
- The information governance team will maintain a log of contracts reviewed for information governance compliance.
- All contractors who are processing the Trust's data on our behalf must comply with information governance requirements.

- Contractors who are providing a service to the Trust and either require access to the Trust's information assets (remote or on site) or will have access to Trust information because they are working on site must comply with information governance requirements.
- The IG team will audit data processor contractors for compliance with information governance requirements every two years.
- Information governance must approve all system access requests for third party contractors.

51 Third party remote access

Where an application is supplied by a third party organisation access may be required remotely to the application by the third party in order to deal with a technical fault, run a maintenance programme or upgrade the version of the application.

All third party organisations that require remote access to their applications require:

- information governance approval – please refer to the information governance operational manual
- if individuals from the organisation require a domain account and application/ system access then information governance approval is also required for the system access – please refer to the information governance operational manual
- a record of third party organisations that have been approved for remote access will be held on the information asset register
- if a third party requires remote access generic accounts, information governance approval must be obtained, key users will still be required to have individual access tokens with generic accounts used for on call and additional support
- contractors are required to keep a log of when they have accessed the Trust servers, who has accessed and why

52 Third party PC equipment connected to Trust network

The connection of any third party PC equipment to the Trust network is not allowed, the default must be to use to the Trust issued PC equipment, such as desktop PCs and laptops.

Where this is not possible an exception to this policy must be applied for, all exceptions must be approved by information governance and IT. Exceptions will only be granted where there is a justifiable business requirement and the third

party can demonstrate compliance with the 'standards for connecting non HP PCs to the network'.

Systems lifecycle

53 Disposal of equipment and paper

All computer hardware equipment, devices and confidential/PID paper must be disposed of securely.

- All old IT hardware must be returned to IT for disposal including PCs, laptops, tablets, printers, keyboards, display equipment, screens, scanners, servers and hard drives.
- HP devices that require collection, place a request using the service catalogue request or by contacting the service desk on extension 257257.
- All other IT equipment please contact estates on extension 216696 to arrange collection.
- Digital dictaphones, videos, cameras, digital image storage devices, answering machines and other audio recording devices must be returned to estates for disposal, contact extension 216696 to arrange collection.
- Confidential/ PID paper must not be placed in waste bins, it must be shredded or placed in confidential bins.
- Mobile devices including tapes, CDs/DVDs, PDAs, floppy disks, USBs must be placed in the disposal bins provided in medical records, IT and the management offices.
- Fax rolls and bar code labels must be placed in the bins provided across the Trust.
- Mobile/ smart phones must be returned to voice services for disposal.
- Trust Blackberries must be returned to the information governance team for disposal.
- Medical equipment must be disposed of as per management of medical devices policy.
- The information governance team are responsible for monitoring the secure destruction of equipment and paper.

Please also refer to the waste disposal procedure and the waste management policy.

54 Decommissioning of systems

- Comply with decommissioning procedure/ checklist.
- Patient identifiable data must be archived to LARDR.
- The IAO for the system is accountable for identifying, planning, authorising, executing and signing-off any decommissioning activity.
- Preliminary information gathering about the system in question should be undertaken according to the requirements outlined in the information systems decommissioning procedure.
- A decommissioning plan should be prepared containing details as outlined in the information systems decommissioning procedure.
- If data or system migration is to be carried out, a migration plan should be included in the decommission plan.
- The decommissioning plan should pay particular attention to data management, especially where PID is present. The decommissioning plan should be signed off by IG.
- Where data is to be archived or migrated, the Trust-wide and local department data retention schedules should be complied with.
- For live systems, the impact of the decommissioning should be assessed and risks mitigated as necessary.
- All of the four basic decommissioning steps outlined in the information systems decommissioning procedure should be evidenced in documentation and be kept for future reference and audit purposes.

General

55 Monitoring compliance with and the effectiveness of this document

Key standards:

- new systems and processes comply with information governance requirements
- third party contracts comply with information governance requirements
- information risk assessments are in place to manage information risks
- the trust complies with the requirement to meet minimum level 2 standard in the information governance toolkit assessment
- staff attend information governance training and sign compliance with the information governance code of conduct

The standards will be monitored by the information governance team by:

- submission of evidence required on a yearly basis as part of the information governance toolkit
- completion of information governance audits in all areas, producing a report and action plan. The IGSG will receive a yearly report in March highlighting the findings of the audits
- information governance quarterly report monitors key standards for information governance such as incidents, freedom of information requests and data quality
- a log will be maintained of all new system/ processes information governance actions
- a log will be maintained of all third party contract information governance actions

The IGSG is responsible for monitoring compliance with information governance and ensuring that the necessary actions are undertaken.

56 References

Information Governance Toolkit
Data Protection Act 2018
NHS Confidentiality Code of Practice
NHS Records Management Code of Practice
NHS Information Security Code of Practice

57 Associated documents

- audit access to patient records in Epic
- business continuity (BC) planning
- confidentiality of personal health information
- data protection
- disciplinary
- equality, diversity and inclusion in employment
- freedom of information
- grievance and dignity at work
- information governance incident and investigation
- information risk assessment
- information systems decommissioning
- management of medical devices
- mobile phones and other mobile communications equipment
- records management
- records: preservation, retention and destruction
- registration authority
- system-level security
- waste disposal
- waste management

Equality and diversity statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

Disclaimer

It is **your** responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

Document management

Approval:	Information Governance Programme Board, 3 September 2020		
JDTC approval:	N/A		
Owning department:	Information governance		
Author(s):	Michelle Ellerbeck, Information Governance Lead		
Pharmacist:	N/A		
File name:	Information governance and information security policy Version14 September 2020		
Supersedes:	Version 13, July 2017		
Version number:	14	Review date:	September 2023
Local reference:		Document ID:	7494