Information Handling Policy

Author (s)	**Caroline J. Britten** **Head of Information Governance, NHS Leeds Community Healthcare (former)** **Simon Boycott, Head of Development and Governance**
Corporate Lead	**Leeds General Practice Confederation** **Jim Barwick, Chief Executive**
Document Version	**1.2**
Date approved by Quality Committee	**1st August 2023**
Date issued	**1st August 2023**
Review date	**July 2026**

Executive summary

This policy forms part of the overall approach to Information Governance and Information Security and aids our compliance with the Data Security and Protection Toolkit and our statutory obligations under the Data Protection Act (1998). Compliance will safeguard the confidentiality of patients, staff and The Confederation's business operations and reduce organisational risk by helping to mitigate the frequency and severity of confidentiality breaches.

This policy deals with some situations staff in the NHS will encounter when handling the confidential information of patients or staff. Any information that is being processed through transfer must adhere to these policies. It is important to focus not solely on systems and technology, but for all of us to act as a 'Personal Safe Haven' whenever we handle personal, sensitive and confidential information.

The policy has been reviewed and amended in line with current guidance around Information governance and information security.

Contents

1.0 Purpose....4
2.0 Scope....4
3.0 Definitions....4
4.0 Responsibilities....6
5.0 Safe Haven Procedures....7
6.0 Telephones....8
7.0 Fax....9
8.0 Post....9
9.0 Safe Transfer of Paper Records....9
10.0 Emails....12
11.0 Moveable media....12
12.0 Computers....14
13.0 Paper Documents....14
14.0 Buildings and Security....15
15.0 Information Sharing....15
16.0 Sharing information with other organisations (Non NHS)....15
17.0 Copyright....15
18.0 Risk Assessments....15
19.0 Training Needs....15
20.0 Monitoring Compliance and Effectiveness....17
21.0 Approval and Ratification process....18
22.0 Dissemination and Implementation....18
23.0 Review arrangements....18
24.0 Associated The Confederation documents....18
Appendix A....19
Appendix B: Safe Haven label and instructions for Fax transfers....20
Appendix C: Guidance on what to include in a validation process for outgoing mail as a “safety net” for the “letter to wrong address” scenario....21
Appendix D: Fax Disclaimer....22

1.0 Purpose

The Leeds General Practice Confederation (The Confederation) core business often requires the movement of personal, sensitive and otherwise confidential information, it is imperative that the confidentiality of such information is maintained via the use of secure communications methods and staff whose own behaviour enhances our confidentiality culture and information security.

The Confederation is required to have a policy to ensure that the transfer of person identifiable information into and out of The Confederation and within The Confederation between departments and sites is as secure as possible. The policy is intended to meet Caldicott, Data Protection, Statement of Compliance and Data Security and Protection toolkit requirements. It forms part of The Confederations compliance with Principle 7 of the Data Protection Act which states: 'Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss'.
The policy has been updated to reflect the increased access to mobile working solutions and remote access to Trust systems.

2.0 Scope

The policy covers all person identifiable information which may relate to staff, service users, carers, or any individual about whom we hold information.

3.0 Definitions

Record: ISO Standard15489-1:2016 Information and documentation defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. The Data Protection Act 1998 (DPA) S68(2) defines a health record which 'consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'.

Health Record: A health record is any record of information relating to someone's physical or mental health that has been made by (or on behalf of) a health professional.

Personal Information: Information which may in itself, or alongside other information available from additional sources, be used to identify an individual. As defined by the Data Protection Act (1998).

Confidential Information: Personal Information and Sensitive Personal Information are defined by the Data Protection Act (1998), other classes of information should be regarded as confidential and worthy of Safe Haven handling. These include confidential information relating to The Confederation's business interests and activities, personal bank account details of staff and service users and any information which is given 'in confidence' or has the quality of confidentiality.

Anonymised Data: Data with all identifiers removed such that data subjects within cannot be identified. This differs to pseudonymised data, which can be identified using a key. Truly anonymised data cannot be re-identified, even at source.

Safe Haven: A term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within The Confederation to ensure confidential patient or staff information is communicated safely and securely. The 'Safe Haven' concept was first introduced to indicate a fax machine operated in such a way to enhance the confidentiality of personal and sensitive information sent to it. Given the proliferation of other information transport mechanisms, The Confederation approach to Safe Havens must encompass a wider array of communications media.

Data Flow: The path taken by data within a device, network, or organisation, as it moves from its source to a data repository or a data user.

Portable or Moveable Media: is defined as all electronic information that is not held on The Confederation network drives. This includes information held on USB memory sticks, CDs, DVDs, desktops, local hard drives, floppy disks, diagnostic, flash memory cards and other electronic devices capable of holding data. Essentially this is anything you can copy, save and/or write data to which can then be taken away and restored on another computer.

Agile or Mobile Working: A working arrangement where staff no longer operate from a fixed base or office. Staff can operate via remote connection to Trust systems over secure links from mobile / remote locations.

Government Secure Intranet (GSi): A interconnecting secure communications infrastructure, providing secure and encrypted communications channels across the NHS and wider public sector. The HSCN and NHS.net e-mail are part of GSi.

Pseudonymisation: A privacy-enhancing technology intended to produce an identifier which can only re-identify data subjects when the identifier is compared to the pseudonymisation key. Without the key, the data is anonymised.

Person Identifiable Data or Information: "personal data" means data which relate to a living individual who can be identified from the data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Examples include; name, address, date of birth, NHS number, NI number, description, photograph etc.

Sensitive Personal Data or Information – Information relating to race, ethnicity, religion or similar beliefs, sexuality, political affiliation, trade union membership, physical and mental health, and forensic history.

4.0 Responsibilities

4.1 Chief Executive is responsible for signing of appropriate declarations on behalf of The Confederation and will be ultimately accountable for Information Governance issues.

4.2 Senior Information Risk Officer (SIRO)**,** Chief Executive Officer will act as the board-level owner of information risks and be the point of contact for board level input in this area. Progress against this procedure, particularly any difficulties and the resultant risks must be reported to the SIRO.

4.3 Caldicott Guardian will advise on patient data confidentiality matters and provide this expertise as required. .

4.4 Data Protection Officer will be The Confederations first line of Information Governance expertise and act as first point of contact for advice on this policy and the secure movement of confidential information.

4.5 Operational Managers will ensure that:

- appropriate arrangements are in place to manage post, e-mail and telephone calls in accordance with the policy.
- all fax machines are appropriately labelled in line with the policy and that the fax disclaimer is available on cover sheets.
- all staff are made aware of the provisions in this policy at induction and that refreshers briefings are available through the Information Governance Department
- Non compliance of the policy can be investigated and may lead to disciplinary action.

4.6 Staff are responsible for ensuring they comply with this policy along with specific professional codes of practice for their disciplines, this incudes attendance for all identified training and reporting any incidents of non-compliance via the Datix® Incident Reporting System

All staff employed by, and working on behalf of The Leeds General Practice Confederation must work in concordance with the Leeds Safeguarding Multi-agency Policies and Procedures and local guidelines in relation to any safeguarding concerns they have for service users and the public with whom they are in contact.

4.7 Information Governance (IG) Group is responsible for monitoring and reviewing arrangements for this policy.

5.0 Safe Haven Procedures

The Confederation accepts there is a wealth of routine communication, by paper and electronic means, which happens during the normal course of clinical and business operations.

All staff should communicate in a manner which is both appropriate and proportional in security to the content of the material they are sending. We are all responsible for the decisions we make regarding the confidentiality of our data and its storage and transfer. Further guidance should always be sought if staff members are unsure from their line manager or the Information Governance Department.

5.1 Personal Safe Haven Working

The most important aspect of information security is the ‘Human Element’. It is not sufficient to simply consider systems, devices and working practices as the entire scope of the Safe Haven concept, particularly with the advent of mobile / remote access and agile working arrangements. All staff must adopt working practices so that they can be considered a ‘Personal Safe Haven’ – essentially a safe pair of hands for personal, sensitive or confidential information.

Basic and common sense steps will help us all to meet this important obligation:-

- Maintain an awareness of your surroundings and the threats to information security in your immediate vicinity.
- Ensure PCs are locked or switched off when not in use.
- Make sure that PC screens are not inappropriately viewed by 3rd parties, particularly when working remotely.

- Ensure information is not visible or accessible to inappropriate people.
- Clear desks and other workspaces of information when leaving a workstation.
- Ensure that information transferred between locations arrives intact, without total or partial loss en-route.
- Store information in the boot of a car when in transit.
- Remove personal, sensitive or confidential information from any vehicle on arrival at your work base, home, or final location.
- Only take & use personal, sensitive or confidential information when working from home with the authorisation of your line manager.
- When working from home, ensure that information is used and stored securely and protected from access by family members or other visitors to your home at all times.
- Check the fax number before sending information via fax, particularly when using preset or speed-dial numbers.
- Ensure that e-mail addresses are correct before sending information via any e-mail method, particularly when addresses are auto-completed by your e-mail software.
- Know and apply the key Caldicott Principles to any information you are intending to send.
- Facilitate mobile / remote / agile working via secure method (NHS.net e-mail, encrypted memory stick, encrypted laptop etc.). **NEVER** do this by e-mailing personal, sensitive or confidential information to a private / personal e-mail account or by storage on a non-Trust PC or laptop.

6.0 Telephones

6.1 Telephone Calls

6.1.2 Do not make sensitive telephone calls where you can be overheard e.g. Reception

6.1.3 When receiving a call check to ensure you are speaking to the correct person, ring back (where possible) to confirm someone’s identity.

6.1.4 It is appreciated that when patients are being treated on inpatient unit’s family members will want to know about their relatives and friends. On inpatient units, staff must only give general information or to confirm that the individual is on the unit and their general condition without reference to the exact illness or treatments. If the patient consents, then more information can be shared.

6.1.5 Where a celebrity is receiving treatment staff are advised to contract The Confederation security officer in the estates team and the communications team to discuss how to disclose information to those who are not related to the patient.

6.2 Welcome Messages

When a call is made to a service operating from a hub the message given at the start of the call clearly advise patients that their calls are being recorded for training and quality purposes.

6.3 Answer phones

Where an answer phone is receiving messages which may be confidential e.g. an out of hours job application phone, where callers leave names and addresses the messages must be recorded and transcribed in a location where they cannot be overheard by unauthorised staff. The answer phone must be protected by pin number access or being in a locked room when unattended to prevent unauthorised access.

6.4 Leaving Telephone Messages

Where information is of a confidential nature it should be given over the telephone only to the intended recipient or their agreed representative. Messages must not be left on answer phones unless this is the specific agreement. The person making the call will always check if it is convenient for the recipient to receive the information before passing it on. The intended recipient should be asked for by name, assumptions should not be made that the person answering the phone is the intended recipient. Calls should not be made where they may be overheard by unauthorised individuals when passing on or receiving confidential information.

Where an unfamiliar caller is seeking information, care should be taken to ensure that the caller is genuine, by taking a number and calling back after checking it.

7.0 Fax

Fax machines must not be used in Confederation Services.

8.0 Post

8.1 Incoming mail should be opened away from public areas.

8.2 Outgoing mail (both internal and external) should be sealed securely and marked private and confidential if it contains person-identifiable information. Where possible send post to a named person. See Section 9 for safe transfer of paper records.

9.0 Safe Transfer of Paper Records

The Confederation requires that all information including paper records which contain clinical information is sent according to procedures described below.

9.1 Information taken away from Confederation premises

9.1.1 Staff must consider the need for taking paper patient/client/staff records out of their base with them on a visit. This must only happen when absolutely essential and there is no other method available for accessing/recording the information required. Staff must not carry around more information than is necessary.

9.1.2 If patient records need to be taken from their base, staff must follow the steps in Figure 2 in order to reduce the risk of the records being accessed by an unauthorised person, lost or stolen.

Figure 2: Procedure to be followed when taking paper patient records out of base
a. Consider if the record is needed in order to carry out the visit. Records must not be removed for general administration purposes, e.g. writing reports.
b. Only take the records for visits that are pre booked.
c. Record the removal and return of files taken away from the workplace
d. Records must be stored and carried in a secure bag/case. Records must not be carried ‘loosely’, as this increases the risk of dropping them and losing something.
e. The bag/case used to store the records must never be left visible in a car when visiting, but accompany staff on each visit/into each home where possible. Records, if left in unattended cars, must be locked in the boot.

f. If not returning to base at the conclusion of visits the records must be stored in the bag/case used and taken out of the car overnight into their home. Care must be taken to ensure that family members or visitors cannot gain access to the records.

g. This practice must only occur if the member of staff is not returning to their base after the working day or the records are required for the next working day. Staff must have the agreement of their manager if it is necessary for them to work in this way.

h. Records must not be away from base for more than one working day i.e. if a member of staff is not returning to base at the conclusion of their working day, the records taken out on visits must be returned on their next normal working day.

i. There may be exceptional circumstances when this is not possible e.g. if a member of staff goes off sick before returning the notes. In this situation, the records must be returned as soon as is practically possible. Managers may have to make arrangements to retrieve records if they are required whilst the member of staff is off for a period of time.

9.2 Transfer of records to other bases in Leeds

9.2.1 Physical handover

Where the record is related to significant events e.g. complaints, legal action, access to records requests, serious incidents; or where the person holding the record or the person asking for it thinks that the record is particularly sensitive for other reasons, it should be delivered in person wherever possible. Loose person identifiable information must not be handed to another person for delivery simply because they are going to the destination department. It should only be delivered if the information is in a sealed envelope, marked as confidential and to a named individual.

9.2.2 Internal Mail - Shuttle

When information or clinical records are sent in the internal mail an assessment must be made as to the risk of loss. If the loss of those records could compromise patient care or create a serious breach of confidence, the steps outlined in Figure 3 must be followed.

Figure 3: Transfer of clinical records using internal mail

a. Where a reception has a recorded delivery book for internal post this must be used to record clinical files and sensitive mail sent in the shuttle creating an audit trail in the unlikely event the post does not arrive at stated destination.

b. Records must be transferred in new unused envelope which can be securely sealed, be clearly addressed to a named individual including their title and location and be marked Private and Confidential. A ‘Return to sender’ address should be put on any postal correspondence.

c. Where bulk transfers (50 records or more) are used the number of items in transit must be recorded with a method to identify any records that are transferred. The sender must add their name, title and location to the back of the envelope, to allow undelivered post to be returned. A note must be attached to the records asking the recipient to contact the sender to acknowledge receipt. This can be done via email, telephone or by a return receipt. Alternatively an email can be sent to the recipient telling them the records are in transit and to contact the sender if they do not arrive within three days

d. If the sender has not heard from the mail's designated recipient after three working days they must contact the recipient, to check receipt. Undelivered post must be reported as an incident using the Datix® incident reporting system if after a further 7 days the post has not arrived.

e. If possible, staff should nominate a colleague to open mail containing service user records when on planned or unplanned leave. Such records must be kept secure until the member of staff returns from leave.

f. If staff need to send records urgently then they must contact the intended recipient in advance to ensure that they are not on leave or working away from their base.

9.2.3 External Mail - Royal Mail

When information or clinical records are sent in the external mail an assessment must be made as to the risk of loss, with external mail avoided in most circumstances for sending clinical records to health centres in Leeds. If the loss of those records could compromise patient care or create a serious breach of confidence, the steps outlined in Figure 4 must be followed.

Figure 4: Transfer of clinical records using external mail

- **Where original records or copies have to be sent to organisations outside Leeds, they must be securely sealed and addressed as for internal mail [Figure 3: b] and be sent using Royal Mail's Recorded Delivery service which provides a tracking and tracing service.**

Where bulk transfers (50 records or more) are used, the number of items in transit must be recorded with a method to identify any records that are transferred.

9.2.4 Tracking records

Where there has been an identified risk that loss of the information or clinical record could compromise patient care or create a serious breach of confidence as part of the above procedures the record must be tracked. In these situations the person responsible for sending or taking records must log:

- The name and type of records removed, including any unique identifying number
- The reason for removal and whether likely to be temporary or permanent if known
- The date of removal
- The person the record is being sent / handed over to
- Method of transfer
- The date notified that the records have arrived at their destination including name

of person confirming receipt, if appropriate.
- The date records return to base, if appropriate.

Where data is received in an insecure manner from a sender i.e. does not follow this policy, the recipient will notify the sender and report as an incident. They should then request that any future information must be sent securely.

10.0 Emails

10.1 To and from patients

Email is an unsecure means of communication, with emails sent to and from patients that are not encrypted a possible Data Protection Act breach. Patients may initiate communication with staff as part of their treatment. If a patient initiates such communication it can be considered that they have consented to communication by email even though it is not a secure means of communication. However it is advisable for a patient to be sent an email explaining that emails are insecure and before further emails can be exchanged they must consent to receive further emails. Consent to receive communication by email must be documented on the patient record.

10.2 System monitoring

All emails are monitored for viruses. All email traffic (incoming and outgoing) is logged automatically. These logs are audited periodically. The content of emails is not routinely monitored. The Confederation reserves the right to retain message content as required to meet legal and statutory obligations.

11.0 Moveable media

All moveable media used on information systems owned or operated by The Confederation are covered by these guidelines. Moveable media can include:

- Tapes, including audiotyping tapes;
- Floppy disks,
- Removable or external hard disk drives,
- Optical disks i.e.: DVD and CD,
- Solid state memory devices including memory cards, pen drives, memory sticks etc.
- Any electronic information held outside of The Confederation network drives.
- Smartphones
- Digital cameras
- Dictaphones
- Diagnostic equipment with internal storage
- Laptops or tablet devices

11.1 Laptops

Laptops are classed as moveable media and covered by this policy although they have been encrypted. All laptops must be encrypted even if the laptop is only to be used for remote access to network. The policy does not inhibit the use of person-identifiable or business sensitive information however it must not be downloaded held or transferred on moveable media unless that media has been encrypted. When travelling, laptops must not be carried in open view and must be removed from sight and not left in the car once the journey is complete. If laptops are taken home by staff they must be kept safely and securely. This means that other members of their family and/or their friends/colleagues must not be able to access or use the laptop.

11.2 Data Storage Devices

Data storage devices e.g. Hard Drives, Memory Sticks, CD’s, DVD’s, PDA’s or mobile telephones. All devices containing person-identifiable or business sensitive information must be encrypted to NHS standards using encryption provided by The Confederation.

NEVER email personal, sensitive or confidential information to a private / personal email account or store personal, sensitive or confidential information on a non-Confederation PC or laptop.

Using personal devices for recording, storing or transporting personal, sensitive or confidential information data is not permitted and can lead to disciplinary action.

11.3 Risks Associated With Moveable Media

11.3.1 Disclosure of data

The nature and size of moveable media is such that they are prone to accidental loss and /or theft which could result in accidental, negligent or intentional disclosure of data. Unauthorised disclosure of sensitive information, along with the obvious potential of public embarrassment to The Confederation, could occur if an item of moveable media fell into the wrong hands.

11.3.2 Infection of PCs – Malicious software

Computer users can save vast amounts of data on moveable high capacity media devices and can very easily transport data and possibly unwittingly malicious software between PC systems and associated networks. Examples of malicious software include Virus Programs, Trojan Horses and malicious programs designed to deny access of service. Moveable media can be susceptible to data loss or corruption so it is advised users take care in what is stored on them. Some devices will create additional drive letters on the host computer which can be confusing and lead to accidental deletion of data on a valid drive.

11.3.3 Security of Data

Data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up. Therefore, moveable media must not be the only place where data obtained for work purposes is held. Copies of the data must also remain on the source system or computer until the data is successfully transferred to another computer or system. All moveable media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption. Moveable media must also be physically protected against damage, abuse or misuse when used, where stored and in transit. Whenever data is transferred between equipment there are the risks of contamination being introduced onto the network or equipment. This could affect the integrity of the data itself, the hardware and other data assets and The Confederation, if the data is lost or used inappropriately. All staff are responsible for the appropriate use and security of data and for not allowing moveable media to be compromised in any way whilst in their care or under their control.

11.3.4 Loss of any moveable media

It is the duty of all staff to report immediately any actual or suspected loss, misuse or irresponsible actions in the use of moveable media to the computer helpdesk.

Currently the email is computer.helpdesk@nhs.net. The incident must be reported as an incident using the Datix® incident reporting system

12.0 Computers

12.1 Do not share log-ons and passwords with anyone

12.2 Do not share smartcards or leave smartcards unattended

12.3 Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data. PCs or laptops must be locked or switched off when you are away from your desk for any length of time.

12.4 Information must be held on the organisation’s network servers, not stored on local hard drives such as the c drive or the desktop or removable media. Information must not be saved or copied into any PC or media that is “outside the NHS” unless there is a lawful basis to share the information.

12.5 All person-identifiable information sent by email must be sent from one NHSmail address to another secure e mail domain such as NHS.net to NHS.net or via an encrypted attachment e.g. firstname.last name@leeds.gcsx.gov.uk See Appendix C.

12.6 The Confederation reserves the right to inspect (or in the case of encrypted data files, verify with the user of) any and all files stored in private areas of its network or on local hard drives in order to ensure compliance with this policy.

13.0 Paper Documents

13.1 All sensitive records must be stored face down in transit through public areas and not left unsupervised at any time.

13.2 Information that is no longer required (e.g. post it notes, messages) must be shredded or disposed of in the confidential waste.

13.3 Ensure that documents are properly ‘booked out’ of any filing system (if necessary). Copies should be sent or retained, as appropriate. See Section 10 for safe transfer of paper records.

13.4 If a single staff member is responsible for a case then they are also responsible for the confidentiality and security of those records in their possession.

14.0 Buildings and Security

14.1 Do not allow unauthorised people into areas where confidential information is kept unless supervised. Check peoples ID badges and question anyone you believe may not be authorised to access the building.

14.2 Take measures to prevent casual sight of information. Keep a clear desk or ensure that no confidential information is left out when the desk is not in use. Store person identifiable information in a locked drawer or filing cabinet when not in use.

15.0 Information Sharing

Where information is routinely shared with a third party organisation an information sharing agreement may be required which specifies the purpose and the method of sharing the information. Information Sharing Agreements must be agreed and signed by the Caldicott Guardian. Further information about sharing agreements and whether one may be required for your data flow can be obtained from the Information Governance Department.

16.0 Sharing information with other organisations (Non NHS)

Staff sharing personal information with other agencies must be aware of the Leeds Inter-agency Information Sharing Protocol or other sharing arrangement and the requirement to have an Information Sharing Agreement in place for the routine sharing of person identifiable information. This will provide The Leeds General Practice Confederation with the assurance that these organisations are able to comply with the safe haven ethos and meet legislative and related guidance requirements.

17.0 Copyright

Under the Copyright Designs and Patents Act 1988, copyright law can be infringed by making an electronic copy or “transient” copy (which occurs when sending an email.) Copyright infringement is becoming more commonplace as more and more people forward text, graphics, movies and audio clips by email. Employees must not therefore copy; forward or otherwise disseminate third-party work without appropriate consent.

18.0 Risk Assessments

Risks identified with the implementation of this policy have been assessed and mitigated as far as possible, in line with The Confederations risk appetite. Should any further risks be identified following implementation, these will be assessed and consideration will be given to an urgent review/revision of the policy (and procedure). All The Confederation staff must report all incidents involving noncompliance of this policy via the Datix® incident reporting system.

19.0 Training Needs

The Confederation implements a structured programme of training based on a training needs analysis. The Information Governance Lead will ensure that training is provided as appropriate.

All staff will complete annual Information Governance training as prescribed via ESR. Bespoke training and development is available to all teams and services tailored to their specific needs.

All training is recorded and monitored through the workforce development department, which reports non-attendance to line managers.

Refer to the Statutory and Mandatory Training Policy including Training Needs Analysis. Up to date information is available on the Intranet for course details.

20.0 Monitoring Compliance and Effectiveness

Minimum requirement to be monitored / audited	Process for monitoring / audit	Lead for the monitoring / audit of Process	Frequency of monitoring / auditing	Lead for reviewing results	Lead for developing / reviewing action plan	Lead for monitoring action plan
Incidents	Datix	Head of Operations	Monthly	Quality Committee	Quality Committee	**Quality Committee**
Breaches of Confidentiality	Datix	Head of Operations	Monthly	Quality Committee	Quality Committee	**Quality Committee**
Reportable Incidents (ICO)	**Mandatory Reporting Tool (NHS Digital)**	**Head of Operations**	**Monthly**	**Quality Committee**	**Quality Committee**	**Quality Committee**

21.0 Approval and Ratification process

The policy has been approved and ratified by the Quality Committee.

22.0 Dissemination and Implementation

Dissemination of this policy will be via the Confederation website
Implementation will require:

- Operational Directors/ Heads of Service/General Managers to ensure staff have access to this policy and understand their responsibilities for implementing it into practice
- Workforce and the Quality and Professional Developments will provide appropriate support and advice to staff on the implementation of this policy

23.0 Review arrangements

This policy will be reviewed in three years following ratification by the author or sooner if there is a local or national requirement.

24.0 Associated The Confederation documents

- Records Management Policy
- Confidentiality Code of Conduct
- Network Security Policy

Appendix A

Guidance on the use of email

The Confederation Acceptable Use policy states that e-mails across or external to The Confederation network should not contain personally identifiable information because they are not encrypted. Setting up password protection does not provide encryption and does not provide secure transfer of information. any member of staff who needs to routinely receive or send by e-mail person identifiable information should have an nhs.net e-mail account. NHS.net e-mail is automatically encrypted in transit, therefore any e-mail sent from one NHS.net mail account to another (e.g. xxx@nhs.net to yyy@nhs.net) is secure.

NHS.net e-mail is hosted on the N3 network and as such forms part of the wider public sector Government Secure Intranet (GSi). This means that we can also be assured that e-mail is encrypted when delivered to any of the following e-mail domains:-

Secure email domains in Central Government:
- *.gsi.gov.uk
- *.gse.gov.uk
- *.gsx.gov.uk

The Police National Network/Criminal Justice Services secure email domains:
- *.police.uk
- *.pnn.police.uk
- *.scn.gov.uk
- *.cjsm.net

Secure email domains in Local Government/Social Services:
- *.gcsx.gov.uk

E-mail sent to / from NHS.net addresses and e-mail addresses ending in the above will be secure in transit. The Government is expanding GSi coverage and access to other public sector organisations and the list above may increase.

NHS.net mail should not be confused with other NHS e-mail addresses ending with NHS.UK. These addresses are not secure when sending from NHS.net accounts.

When sending outside the GSi network, personal, sensitive and confidential information must be removed from the subject line and body text of the document and sent as an encrypted attachment.

Appendix B

Not used.

Appendix C – Guidance on what to include in a validation process for outgoing mail as a “safety net” for the “letter to wrong address” scenario.

- NEVER overtype existing letters (the obvious pitfall of a change of address indicates why)

- Use an automated footer with page numbering (1 of 7, 2 of 7 etc.) – so you know you are looking for 7 pages and put 7 pages in the envelope!

- Deploy secure print on multi-function device or shared printers so people have to enter a code to get their work – then print jobs do not become inter-mingled.

- Put posters above shared printers / multi-function devices – “STOP – make sure you’ve only picked up your documents – not someone else’s!”

- Build the requirement to check addresses from the Patient Administration System – Carenotes, RiO and SystmOne, or paper record before posting.

- Use the SPINE to corroborate addresses, and act on any discrepancy between local records and the Patient Demographic Service (note: PDS isn’t necessarily right – but it should bring a moment of pause if it’s different to your records).

- Have staff check addresses at clinics/appointments.

- Put posters in reception areas advertising the need for patients to tell us address changes.

- Windowed envelopes remove the necessity for the address to also be written on the envelope too.

- Draft your procedure or process, once corrected, as a simple, fool-proof 1-page document and make it common knowledge in your admin pools.

- Assess any breach against the procedure, and if it uncovers a new flaw, correct it, or take action against staff where breaches occur because it hasn’t been followed.

Staff know best where their own processes have weaknesses – it uncovers situations like “sometimes the file isn’t always available” – this can be addressed as a flaw in the process.

Appendix D

Not Used.

Policy Consultation Process

Title of Document	**Information Handling Policy**
Author (s)	**Previous authors:** **Richard Birmingham, The Confederation Information Governance Lead** **Darren Riggs, The Confederation Information Governance Lead** **Caroline Britten** **Simon Boycott**
New / Revised Document	**Revised**
Lists of persons involved in developing the policy	**Simon Boycott**
List of persons involved in the consultation process	**Quality Committee**