Secure Transfer of Personal Information Policy

Policy information

Policy number: 275

Classification:
Corporate

Supersedes:
N/A

Local Safety Standard for Invasive Procedures (LOCSSIP) reference:
N/A

National Safety Standards for Invasive Procedures (NatSSIPs) standards:
N/A

Version number:
V.4

Date of Equality Impact Assessment:
Detail date of EqIA

Approval information

Approved by: Sustainable Resources Committee

Date of approval:
28/02/2023

Date made active:
06/06/2023

Review date:
28/02/2026

Summary of document:
This policy lays out the security requirements for the transfer of personal information into, across and out of the Health Board in any format.

Scope:
This policy applies to all staff and service areas across the Health Board.
It applies to all hard copy and electronic personal information processed by the Health Board.

To be read in conjunction with:
837 - All Wales Information Security Policy (opens in new tab)
172 - Confidentiality Policy (opens in new tab)
224 - Information Classification Policy (opens in new tab)
836 - All Wales Information Governance Policy (opens in new tab)
291 - Personal Employee Records Management Policy (opens in new tab)
201 - All Wales Disciplinary Procedure and Policy (opens in new tab)
494 - All Wales Email Use Policy (opens in new tab)

Patient information:
Include links to Patient Information Library

Owning group:
IGSC

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:

Reviews and updates		
Version no:	Summary of Amendments:	Date Approved:
1	New Policy	May 2012
2	Updated Policy following review	22.08.2017
3	Updated – Data Protection Act 2018/UK General Data Protection Regulation or any subsequent legislation to the same effect	26.06.2018
4	Revised and Updated	Feb 2023

Keywords
Information Governance, Information Security, Personal Information

Glossary of terms

Provide a glossary of terms and abbreviations

Term	Definition
Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. They uphold the Caldicott Principles that lay out how patient information should be handled by NHS organisations to ensure confidentiality is upheld.
Bulk Transfer	The transfer of electronic or paper information that is 'batched up' to be sent out of a location and/or organisation and involves sending personal information about more than 10 individuals.
Data Protection Legislation	Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared.
Encryption	Is the process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Information Asset Owner	Every information asset must be assigned an owner within the Health Board who will be responsible for it throughout its lifecycle. This Owner may work in any department but must have sufficient ability, authority and experience to understand the contents and approve the processing of the record
Personal Data	Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person's name and address, an online profile, a member of staff's HR record or records relating to individual's such as patients or service users.
Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Removable Media	Is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs/DVDs, USB flash memory sticks or pens, PDAs, tablets, and smart phones/devices
Requester	Any individual that requests records from a Health Board department / service. They may be another Health Board department / service, a Service provider, an Integrated Services Team, or an external Agency.
Sender	The individual acting for the Health Board that initiates a Data Transfer/sends information. They must have the authority and sufficient knowledge of the nature of the information to determine whether it should be sent and that it is sent securely. Where the final actual task is delegated to administrative, untrained or

	inexperienced staff, the original Sender remains responsible for ensuring the Transfer complies with this policy
Senior Information Risk Owner (SIRO)	An Executive Director or member of the Senior Management Board with overall responsibility for information risk across the Health Board.
Special Category Data	Special category data means personal data consisting of information as to: - Genetic and biometric data - Political opinions - Religious or other beliefs - Trade union membership - Physical or mental health/condition - Sexual life And although not specifically described as special category data, this information requires the same treatment: - The commission or alleged commission of any offence - Any proceedings for any offence committed/alleged to have been committed, the disposal of such proceedings or the sentence of such proceedings
Unauthorised Access	Access to information that is not part of your work duties. Access to a patients record where the patient is not under your care.

Contents

Introduction

The sharing of information between departments within the Health Board, to third-party service providers, to other public bodies, commercial organisations and individuals is an important part of delivering safe and effective patient care and for the effective running of the Health Board.

Although information sharing is an important part of what the Health Board does, all staff need to make sure that it is done safely, legally and in a way that ensures confidentiality at all times.

In every transfer of information there is a risk that the information may be lost, misappropriated or accidentally released. The Health Board has a legal and moral duty of care when handling information, particularly that containing personal and/or confidential information belonging to our patients and staff.

Policy statement

The organisation recognises its responsibility to process its personal information correctly and in-line with all legal, regulatory and internal policy requirements.

Scope

This policy provides information to all staff about the minimum security requirements they must use when transferring information into, across and out of the organisation, via any media and in any format. This policy applies to all employees of the Health Board, volunteers, any contracted staff and third-party organisations that processes the organisation's information.

Aim

This policy outlines the responsibilities and the minimum security requirements for the transfer of personal information and should be read and understood by all staff and third parties that use and transfer Health Board information.

The correct application of this policy will ensure that the Health Board is compliant with its legislative responsibilities including the Data Protection Act 2018/UK General Data Protection Regulation or any subsequent legislation to the same effect, reduce the risk of an information security breach taking place and provide assurance to our staff and patients that information assets are being properly managed.

Objectives

The aim of this document will be achieved by the following objectives:

- Ensure that staff understand their responsibilities and the most appropriate methods for transferring and sharing information.
- Protect and prevent personal or confidential information from being lost, stolen or intercepted by unauthorised persons.
- Reduce the risk of an information security breach from taking place.
- Maintain patient and staff trust in the Health Board that their personal information is being managed safely and appropriately by staff across the organisation.
- Ensure that access to information is maintained by preventing information from being lost or stolen or sent to the wrong individual or location.
- Ensure the Health Board is meeting its legal and moral duties in relation to maintaining confidentiality in line with the Data Protection Act 2018/UK General Data Protection Regulation

or any subsequent legislation to the same effect, the Common Law Duty of Confidentiality, the Human Rights Act 2015 and other legislative requirements.

Main body

1. Risks in transferring Personal Information

There are a number of risks associated with transferring personal information.

The severity and type of these risks will vary depending on the method of transfer. Examples of such risks include:

- Information being lost, damaged or intercepted in transit e.g. stolen laptops, lost memory sticks, opened envelopes.
- Delivery service delivering mail incorrectly.
- Information being sent to the wrong address via e-mail, post or fax.
- Information received by the organisation but not delivered to the correct person.
- Personal information not being disposed of appropriately.
- Personal information being deliberately transferred with criminal/fraudulent intent e.g. ID theft.
- Personal information being uploaded to public cloud services such as Dropbox, Google Drive and iCloud which maybe unencrypted and stored in countries without the same regulatory framework as the UK.

Where such risks are realised and personal information is compromised there is an impact on the following:

Individuals - whose information has been put at risk:
Loss of personal information can cause harm and severe distress to individuals, particularly where it is sensitive and private information (special category data) e.g. about their health and care. Loss of information could also have a direct impact on patient care if it is not readily available to the care team. Individuals could also be the victims of identify fraud or other types of crime if their personal information is lost or stolen.
Staff - whose actions placed the information at risk:
Staff who have breached this policy could potentially face disciplinary action. There may also be legal implications and potential criminal action taken if they have knowingly breached key legislation.
The Organisation - whose actions placed the information at risk:
The Health Board may experience a loss of trust, confidence or reputation from the patients/clients, service users, staff, volunteers, partners, contracted staff and visitors, who we rely upon to share information with us to provide a quality and safe service. The organisation could also face a potential fine from the regulator (the Information Commissioners Office) if we do not properly look after and safeguard personal information.

If any staff member has concerns about how information is being sent, shared or transferred within the Health Board they should report this to the Information Governance Team as soon as possible so that appropriate action can be taken.

2. Use of Caldicott and Data Protection Principles when transferring personal information

Before transferring any personal information the Principles should be applied. These are:

Caldicott Principles		Data Protection Act 2018 Principles	
Number	**Principle**	**Article**	**Principle**
1	Justify the purpose(s) for using confidential information.	5(1)(b)	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation').
2	Use confidential information only when it is necessary.	5(1)(b) 5(1)(c)	As above, and Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
3	Use the minimum necessary confidential information.		
4	Access to confidential information should be on a strict need-to-know basis.	5(1)(f)	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
5	Everyone with access to confidential information should be aware of their responsibilities.		
6	Comply with the law.	5(1)(a)	Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency').
7	The duty to share information for individual care is as important as the duty to protect patient confidentiality.	5(1)(b)	As above
8	Inform patients and service users about how their confidential information is used.	5(1)(a)	As above
		Additional Principles - Data Protection Act 2018	
		5(1)(d)	Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
		5(1)(e)	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation').
		5(2)	The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

This policy will assist staff in meeting these principles when sending and transferring personal information.

3. General requirements for transferring personal information

Before sending or transferring any personal information, the sender must consider the various methods available and whether these are appropriate for the type of information being sent.

This policy sets out the main methods / media that can be used for transferring or sending personal information and the minimum requirements that must be followed.

If any staff members are unsure about what method to use for sending or transferring information they can contact their line manager, Head of Department or the Information Governance Team for further advice.

For all transfers of all personal information it is essential that the identity and authorisation of the recipient has been appropriately authenticated by the sender.

This includes taking the following action:

- Double checking any information sent by post to make sure you have the correct name and address. Check these are up to date against any central patient administration systems if appropriate.
- Before putting any information into an envelope to send to another individual, double check to make sure it contains no other information that should not be sent to that person – mixing up of paperwork for different individuals is a common mistake made by staff and can lead to a serious personal data breach.
- Before you send any personal information by e-mail double check you have the correct recipient/e-mail address selected. Double check that the attachments are correct before you press send.
- If sending email communication outside of the Health Board to multiple recipients use the BCC functionality so you do not share individuals' email addresses

3.1. Bulk Transfer

It is essential that all departments of the Health Board have in place systems to ensure that bulk transfers of personal information are appropriately controlled and carried out securely. Bulk transfers are any situation where a department is sending or transferring information about more than ten individuals at the same time.

Any bulk transfer of information should be authorised by your Line Manager / Head of Department for the information being sent. They will decide whether to authorise the transfer of this information after careful consideration of the content, format and method of transfer. They can seek further advice from the Information Governance Team if required about the best method for sending or transferring the information.

The safest way to send a bulk transfer is by setting up a regular file transfer using the Secure File Sharing Portal. All staff can access the portal by following the link and entering their staff Cymru Id and Password. If you have any issues accessing the portal, please log a request to the ICT Service Desk.

Staff can also contact the Information Governance Team for more information about the Secure File Sharing Portal.

3.2. Electronic Mail

Electronic mail should be used in accordance with the Health Board's 491 - All Wales Email Use Policy.

Personal e-mail accounts (e.g. Outlook.com accounts, Gmail, iCloud) must not be used at work for transferring personal information. Additionally no information about patients or staff should be sent to your private email addresses.

The NHS Wales network is considered to be secure for the transfer of any information including PII and business sensitive information. This includes all email addresses in the NHS email directory which include those email addresses typically end in "wales.nhs.uk".

All electronic documents containing personal information and sent outside of the NHS Wales network should be sent using the Secure File Sharing Portal. See point 9 above about how to get access to the Secure File Sharing Portal.

Information sent within the NHS Wales network (anybody with a @wales.nhs.uk e-mail address) can be sent by standard e-mail, unless the information being sent is classified as 'restricted' or 'OFFICIAL – SENSITIVE' information. See the Health Board's 224 - Information Classification Policy for details about the type of information that should be classified as 'restricted' or 'OFFICIAL – SENSITIVE'.

If 'restricted' or 'OFFICIAL – SENSITIVE' information is being transferred or sent by e-mail within the NHS Wales Network then always password protect any attachments as an additional precaution in case the e-mail is sent in error to the wrong recipient. The password should be of organisational standard: 7 characters and a mix of alpha and numeric. Any method for giving the password to the intended recipient should be done via a different method i.e. by telephone, in person etc.

If 'restricted' or 'OFFICIAL – SENSITIVE' information is being transferred or sent by e-mail outside of the NHS Wales Network then always use the Secure File Sharing Portal and upload the information through the 'Packages' option. This is the option used for regular file sharing within the portal.
This means, if you do send the information to the wrong e-mail address in error, you can remove the documents from the folder on the Secure File Sharing Portal (so long as they haven't already been accessed).

In emergencies, If you are unable to access the Secure File Share Portal and the information you need to send is time critical, place all PII in attachments which are encrypted with a password and contact the recipient by phone with the password.

The following checks/precautions should be carried out by the sender at all times when transferring personal information by e-mail:

- Always double check that the name and e-mail address of the recipient are correct. It is good practice to turn off 'auto complete' from your e-mails as this prevents the wrong name and e-mail address being automatically chosen in error.
- The Email message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- Check with the recipient that his / her e-mail system will not filter out or quarantine the transferred file.

- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.
- Ensure that the information within the e-mail is stored in the agreed format for the record type i.e. in line with professional record keeping guidelines. See the Health Board's 224 - Information Classification Policy for further details.

3.3. Electronic Data Transfer (FTP (File Transfer Protocol), Secure FTP)

Standard FTP without encryption is inherently insecure and must not be used for transmitting personal information. Always use the Secure File Sharing Portal when transferring personal information outside of the NHS Wales network.

3.4. Electronic memory and removable devices, (CD, DVD, Floppy, USB drive, Memory Card)

It is always safer to send electronic information using the Secure File Sharing Portal wherever possible. If it is not possible to send or transfer the information via the portal and a removable device needs to be used the following guidance must be followed:

- Personal Information must be enclosed in a file and encrypted using a product approved by the Health Board.
- If the information needs to be posted, it must be sent using an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.
- Any attachment is required to be password protected.
- Any password must be to organisation standard. 7 characters, mix of alpha and numeric.
- Any password to open the attached file must be transferred to the recipient using a different method than email, e.g. a telephone call to an agreed telephone number, closed letter.
- An accompanying message must contain clear instructions on the recipient's responsibilities, and instructions on what to do if they are not the correct recipient.
- Any accompanying messages and the filename must not reveal the contents of the encrypted file.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his/her line manager.

3.5. External and Internal Post/Courier

It is always safer to use the Secure File Sharing Portal to send information to individuals outside the NHS Wales network and this should always be considered as the first option.

If it is not possible to use the Secure File Sharing Portal e.g. you are unable to scan in paper documents to prepare for sending; documents that contain personal information should always be sent using the following methods:

Information classified as being 'confidential'

- **Internal mail to recipients within the Health Board**: If internal mail envelopes are used to send personal information internally, the information must be placed by the sender in a secondary sealed envelope and clearly marked 'Confidential' on the outside of this secondary envelope. Always provide a name and return address on the secondary envelope.

- Send an e-mail or phone the recipient to let them know you have sent them information via the internal mail and ask them to confirm receipt.

- **External mail to recipients outside the Health Board:** Always send information by e-mail using the Secure File Sharing Portal where possible. If this is not possible then always use an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

NB: Only correspondence letters should be sent using standard Royal Mail postage. The name and address of the individual should always be double checked against available systems to ensure it is correct.

Information classified as being 'restricted' or 'OFFICIAL SENSITIVE'

- **Internal mail to recipients within the Health Board:** Staff should always consider scanning in and sending restricted information by e-mail to internal staff within the Health Board. Additional password protection should be applied to any attachments. The use of internal mail for sending restricted information should only be carried out in exceptional circumstances and must be approved by your Head of Department or Information Asset Owner.
- **External mail to recipients outside the Health Board:** Always send information by e-mail using the Secure File Sharing Portal through the 'Packages' option where possible. If this is not possible then always use an approved courier or a secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.

There are a number of standard requirements which must be adhered to when transferring information by post or courier services. There are also additional requirements around removable media and bulk transfers.

3.6 Standard Requirements: Sending or transferring by post

- Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel.
- Mark the envelope/parcel, private and confidential and add a return address and contact details, unless this will directly compromise confidentiality.
- Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit e.g. a tamperproof wallet.
- Always use an approved courier or secure mail method for sending personal information which can be tracked and is signed for e.g. Royal Mail Special Delivery (unless you are sending standard correspondence letters).
- Packages must be received and signed for by the addressee.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.
- When sending Medical Records / Health Care Records copies should be sent whenever possible and the sender must send them in sealed double envelopes with the address on both.

3.7 Standard Requirements: Sending or transferring by removable media using mail/postal services e.g. disks, encrypted memory sticks etc.

When transferring personal information (including bulk transfers) electronically you should always use the Secure File Sharing Portal to complete this task wherever possible.

If you do need to send electronic personal information via other removable media devices then the following should be followed:

- Devices containing information must be sent by an approved courier or a secure mail method which can be tracked and signed for e.g. Royal Mail Special Delivery:
- The individual responsible for passing the information to the Courier, must check the ID of the Courier and obtain a receipt from the Courier when the bulk personal information is collected.
- The sender must confirm the transfer has been received by contacting the recipient.
- The courier must only hand this information over to the recipient or to a nominated individual and obtain a signature when delivered
- Information must be encrypted prior to transfer, in line with Health Board standards.

3.8. In Person

On occasions, personal information may need to be transferred in person. This may be due to the needs of the team or because this may be the most secure method of transferring the information. Examples of this include handing a patient's health care record over to a colleague off site, handing over an encrypted CD of personal data to another organisation etc.

Due to the number of different approaches to transferring personal information in person e.g. on foot, by car, public transport, in electronic or paper formats, it is not possible to give a definitive list of actions to be taken. Careful consideration must be given by the sender and their Head of Department before taking personal information off-site. Any potential risks should be considered and any actions taken to mitigate these risks should be agreed upon and documented.

Information classified as 'restricted' should not be taken off-site unless this has been specifically agreed by the Head of Department and/or Information Asset Owner for the information in question. If 'restricted' information needs to be taken off-site and it is not possible to send it via the Secure File Sharing Portal, this should be done using an encrypted device wherever possible.

Taking paper copies of 'restricted' information off-site should be avoided where ever possible. If it is absolutely necessary to take paper copies off-site, actions need to be agreed to mitigate any risks wherever possible with the Head of Department and/or Information Asset Owner as described above.

3.9. Verbal communications, including telephones

Requests for person-identifiable information from patients or other parties must be verified to confirm the person making the request has a right to know before release of any information.

Person-identifiable information should not be discussed on telephones that have 'hands free' capability unless they are situated in a single user office or car, and only those persons who need the information are present. Headsets should be used in virtual online meetings wherever possible.

3.10. Fax Transmission

Fax is inherently insecure and is not recommended for the transfer of personal information. It is always safer to share information using the internal e-mail system within the NHS Wales network or, the Secure File Sharing Portal to send information outside of the NHS Wales network.

However it is acknowledged that in certain circumstances information will need to be sent by fax. If this is the case the following guidance must be followed in all cases:

- The sender must check that the Fax number is correct and that the receiver is awaiting transmission.
- For personal information the number must be double-checked by a colleague before transmission and telephone contact must be maintained throughout transmission.
- Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine and a clear requirement to securely destroy the message when no longer required.
- The message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her line manager.

Faxes should not be used for sending information classified as 'restricted.' The information should be scanned and sent via the Health Board's Secure File Sharing Portal. Any agreement to use fax for sending 'restricted' information must be agreed by the Information Asset Owner for the information and the SIRO or Caldicott Guardian where patient information is being sent.

3.10 Text messaging (SMS)

There are various potential applications for text messages in the provision of services, e.g. service user appointments. The benefits of using text messages to convey information must be weighed against the risks. Key considerations when using text messages are:

• Is the mobile phone number correct?
• Is the mobile phone receiving the text message being used by the intended recipient of the message?
• Has the message been received, and what provision is there to audit message receipt?

Personal Mobile devices should not be used to communicate with patients.

Text messages should not be used to convey sensitive information and the use of text messages for the transfer of data should be kept to a minimum, e.g. an appointment reminder does not need to include the name of the specific clinic.

No personal information should be sent using SMS without express agreement from the Information Governance Team who will require a privacy impact assessment to be undertaken prior to any sharing of personal information taking place.

3.11. Information Sharing Agreements

All regular sharing of personal information should be subject to the appropriateAgreement (unless the Information Governance Team confirm that an agreement is not required). Further advice and guidance on this can be sought from the Information Governance Team.

3.12. Cloud Storage

Where there is a requirement to share information with others using a cloud storage service, then it is important that individuals who enable the sharing of data do so with the following safeguards:

- Check if the Cloud Storage solution is safe by contacting Information Governance & the Cyber Security Team.
- Once approved as safe grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the correct individuals.
- Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honour all security requirements as well as privacy and confidentiality commitments.

All access to Cloud based storage should be approved by the Information Governance & Cyber Security Team.

4. Responsibilities

Executive Directors

Executive Directors are responsible for the management of information risk within their service areas and are responsible for ensuring their staff and managers are aware of this policy.

The Senior Information Risk Owner and Caldicott Guardian

The Senior Information Risk Owner and Caldicott Guardian are responsible for managing information risk and the safe and ethical use of information across the Health Board and are responsible for ensuring their staff and managers are aware of this policy.

Information Asset Owners

Information Asset Owners are responsible for understanding what information is held within their service areas and for ensuring that this policy is being applied to their information assets by staff and managers.

They are responsible for deciding upon the classification levels of information within their service or information asset area with support from the Information Governance Team where required.

They are responsible for making decisions as to how personal information contained within their information assets and/or sent from their service area should be transferred safely and securely by communicating with staff and managers. Further advice can be sought from the Information Governance Team as required.

They are able to delegate this responsibility to another named individual but they must retain overall responsibility for the information asset and the correct application of this policy to that asset.

Information Governance Team

The Information Governance Team are responsible for disseminating this policy across the Health Board and ensuring it is readily available to all staff. The team are responsible for providing appropriate support and advice to the Information Asset Owners, Service Lead, staff and managers to ensure the policy is understood and adhered to.

Line Managers

Line Managers must ensure that their staff have read and understood this policy and monitor staff compliance in meeting the policy requirements. Line Managers are responsible for reporting the non-compliance of this policy to the Information Governance Team.

All staff

All staff must read, understand and comply with this policy. If a staff member is not clear about any aspect of this policy and its application they are responsible for raising this with their line manager for further clarification.

5. References

- The Data Protection Act 2018/UK General Data Protection Regulation or any subsequent legislation to the same effect
- The Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- Information Commissioner's Office