Data Protection and Confidentiality Policy

Document Control	
Document ID	
Document title	Data Protection and Confidentiality Policy
Version	10
Version status / number	Final
Date ratified	25 April 2023
Approving body	Finance and Audit Committee
Name and job title of lead author	Kathryn Wise, Information Governance Manager
Date published	April 2023
Review date	April 2024

Version Control Sheet

The table below logs the history of the steps in development of the document and detail of where changes were made and why, for example in response to feedback.

Version	Date	Author	Status	Comments
2.0	January 2010	Stephen Rose	Draft	Revision of existing Policy
2.0	February 2010	Stephen Rose	Final	Approved by Information Governance Group
2	16/12/14	V Linford	DRAFT	Circulated to Information Governance Group members
3	23/12/14	V Linford	DRAFT	Comments received from Information Governance Group
4	06/02/15	V Linford	DRAFT	Revised comments from Information Governance Group, amended A&A to F&P
5	10/02/15	V Linford	DRAFT	Incorporation of Confidentiality Audit Procedure
6	19/02/15	V Linford	FINAL	Ratified by F&P Committee
6.1	09/01/17	V Linford	DRAFT	Policy for review. Amendments to committee names only. Caldicott Principle 7 added to Appendix 1
6.2	26/01/17	T Cooper	Draft	Role of Head of Compliance added following initial feedback from Internal Audit of IGT requirements
7	30/01/17	T Cooper	Final	Approved at IGG as changes are minor. For publishing to the intranet
7.1	April 2018	Tracey Cooper	Draft	Policy reviewed to become Data Protection and Confidentiality Policy Additions made to include GDPR and the 6 principles and detail around data protection(p5 and 6) Section on training and monitoring added (p17 -18) Detail around the role of the DPO included.(p7) References to transfers outside the EEA linked back to GDPR and the need to complete a Data Protection Impact Assessment when required p 12 Information Governance Group changed to Data Protection Group and references to IG Toolkit changed p7,16

				Appendix updated to reference Caldicott reviews and updates Shared with DPO, no changes requested
V8	May 2018	Tracey Cooper	Final	Shared with Chair of FP&BC for final approval prior to upload onto the intranet
8.1	May 2020	Dave Britton	Draft	• Formatting changes • Staff roles updated • Key principles grouped together in Section 3 • Further detail added to All Staff responsibilities Sections 9-16 shortened and links added
8.2	July 2020	Dave Brtton	Draft	Updated following following review at DPG and incorporating comments from HR. Detail re-added to sections 9-16 but duplications removed
8.2	August 2020	Dave Britton	Draft	Approved at Finance & Audit Committee
9.0	September 2020	Sue Quinn	Final	Version control and document control updated and requested upload of final version to intranet
9.1	November 2022	Kathryn Wise	Draft	• Minor formatting, spelling and grammar changes • Update to say ratification is from Finance and Audit committee • Updated to show that policy will be on the intranet rather than sent out via safeguarding alert
9.2	December 2022	Kathryn Wise	Draft	Presented and approved at Data Protection Group
9.3	December 2022	Lois Pape, Senior Administrator	Draft	Policy transferred to new template
9.4	March 2023	Kathryn Wise	Draft	Paragraph regarding The Caldicott Guardian added at 3.2
9.5	April 2023	Kathryn Wise	Draft	Policy approved at Finance and Audit Committee
10	May 2023	Lois Pape	FINAL	Document and version control updated. Request upload to intranet.

Contents

Policy 6

Equality Impact Assessment Summary 7

1. Introduction 8

2. Scope 8

3. Responsibilities, accountabilities and duties 8

3.1. The Chief Executive 8

3.2. The Caldicott Guardian 8

3.3. The Data Protection Group 8

3.4. Heads of Service 9

3.5. Information Governance Manager 9

3.6. Data Protection Officer 9

3.7. All staff 9

4. Procedure / implementation 10

4.1. Principles 10

4.2. Data Protection Principles 10

4.3. Caldicott Principles 10

4.4. Common Law Duty of Confidentiality 10

4.5. Using and Disclosing Confidential Patient Information 11

4.6. Ethical Standards 11

4.7. Protecting Information 11

4.8. Physical Security 12

4.9. Physical Transfer of Information 13

4.10. Conversations 14

4.11. Sending Personal Information by Fax 14

4.12. Keeping Computerised Information Safe 15

4.13. Record Keeping Best Practice 17

4.14. Implementation and Dissemination 17

5. Training implications 17

6. Monitoring arrangements 18

7. Links to any associated documents 20

8. References 20

9. Appendices 21

9.1. Information on Caldicott reviews and associated principles. 21
10. Definition of Terms 23

Policy

Spectrum Community Health CIC (Spectrum) provides quality healthcare interventions for people in vulnerable circumstances. We work in partnership to provide primary care, substance misuse and sexual health services, in the community and in secure environments including prisons, hospitals and immigration centres. As a not-for-profit social business, we are committed to addressing health inequalities and investing in the health and wellbeing of the communities we serve.

The aim of this policy is to ensure that all staff understands their obligations with regard to any information held by Spectrum and to ensure that this information is sufficiently protected so that confidentiality is maintained. This includes patient, staff and corporate information.

It aims to ensure that personal data is collected, handled, stored and protected in accordance with Data Protection legislation.

Respect for confidentiality is an essential requirement for the preservation of Spectrum between patients and health care professionals. Without assurances about confidentiality, patients may be reluctant to provide the information that is needed to deliver appropriate levels of care.

Spectrum holds personal information about each staff member and this information must be treated with the same level of protection and confidentiality with which patient information is held.

Equality Impact Assessment Summary

Assessment criteria	Outcome
What is the policy seeking to achieve?	This policy intends to provide clear direction on Data Protection and confidentiality Spectrum CIC
Who will be affected by the policy and why?	All Staff
This policy been written with consideration to	General Data Protection Regulation 25th May 2018 Data Protection Act 2018 Human Rights Act 1998

Impact Analysis

Based on available information, an assessment of the current situation and the changes being proposed, is there a possibility of a different impact (positive or negative) on the groups listed:

Group	Yes / No	Group	Yes / No
Disability	N	Gender reassignment and transgender	N
Gender / Sex	N	Religion or beliefs	N
Race	N	Pregnancy and maternity	N
Age	N	Marriage and Civil Partnerships	N
Sexual Orientation	N	Carers	N

Rationale

This policy has no impact on the above groups

Assessment completed by

Name: Kathryn Wise

Date: 13 December 2022

Procedure

1. Introduction

This document defines the Data Protection and Confidentiality Policy for Spectrum. It applies to all business functions and all information held by Spectrum, in any media or format.

This document:

a) Sets out Spectrum's policy for the protection of all personal data held and maintaining the confidentiality of information.
b) Establishes business and employee responsibilities for data protection and confidentiality
c) Provides reference to legislation and documentation relevant to this policy

2. Scope

The Data Protection and Confidentiality Policy applies to all staff who work for Spectrum (including those on temporary or honorary contracts, secondments, bank staff and students). It also applies to relevant people who support and use these systems.

The Data Protection and Confidentiality Policy is applicable to all areas of Spectrum and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

Confidentiality within independent contractors is the responsibility of the owner/partners. However, Spectrum is committed to supporting independent contractors and will provide advice, share best practice and provide assistance when appropriate.

Failure to adhere to this Policy may result in disciplinary action or referral to the appropriate regulatory body.

3. Responsibilities, accountabilities and duties

3.1. The Chief Executive

The Chief Executive is responsible for ensuring that the necessary support and resources are available for the effective implementation of the Data Protection and Confidentiality Policy.

3.2. The Caldicott Guardian

The director of Nursing is the Caldicott Guardian. The Caldicott Guardian provides leadership and informed guidance on complex matters involving confidentiality and information sharing and ensures that all processing of personal information about those who use the Spectrum's services is undertaken legally, ethically and appropriately and confidentiality is maintained

3.3. The Data Protection Group

The Data Protection Group is responsible for the review and initial approval of the Data Protection Confidentiality Policy. The policy will be ratified by the Finance, Performance and Business Change Committee, in line with Data Security and Protection Toolkit requirements.

3.4. Heads of Service

Heads of Service are responsible for ensuring that they and their staff are adequately trained and are familiar with the content of the Data Protection and Confidentiality Policy.

3.5. Information Governance Manager

The Information Governance Manager is responsible for leading the information compliance agenda within Spectrum supporting both the SIRO and Caldicott Guardian to ensure staff are informed about, and compliant with this policy.

3.6. Data Protection Officer

The organisation has a designated data protection officer. The role is to inform and advise the organisation on its data protection obligations and to monitor compliance with the GDPR and internal policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and conduct related audits

3.7. All staff

All staff must:

- Understand the contents of this policy and associated guidance and procedures and ensure they are compliant with data protection and confidentiality principles.
- Understand fully the purposes for which Spectrum uses personal information to meet its service needs and legal requirements.
- Collect and process information appropriately, and only in accordance with these purposes.
- Complete the mandatory 'Data Security and Awareness' training on ESR within 3 months of commencing employment with Spectrum.
- Report all information security concerns promptly in order that they can be investigated fully.
- On receipt of a request by or on behalf of an individual for information held about them, notify Business Administration so that the request can be responded to within statutory deadlines.
- Understand that breaches of this Policy may result in disciplinary action.
- Know that Section 170(1) of the Data Protection Act 2018 states that it is an offence for a person knowingly or recklessly:
    a) To obtain or disclose personal data without the consent of the controller
    b) To procure the disclosure of personal data to another person without the consent of the controller, or
    c) After obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

4. Procedure / implementation

4.1. Principles

4.2. Data Protection Principles

The organisation processes personal data in accordance with the following data protection principles as outlined in Article 5 of the UK General Data Protection Regulation (UK GDPR).

Personal data must be:

- processed lawfully, fairly and in a transparent manner. (5(1)(a)
- processed only for specified, explicit and legitimate purposes. 5(1)(b)
- processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing. 5(1)(c)
- accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay. 5(1)(d)
- The organisation keeps personal data only for the period necessary for processing. 5(1)(e)
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage 5(1)(f)

The organisation also recognises its responsibility for, and requirement to be able to demonstrate compliance with, the above principles as laid out in Article 5(2), the 'Accountability principle'.

4.3. Caldicott Principles

- Justify the purpose for using confidential information
- Don't use patient identifiable information unless it is absolutely necessary
- Use the minimum necessary patient identifiable information
- Access to patient identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

4.4. Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except as originally understood or with subsequent consent.

In some instances, judgements have been given which recognise a public interest in disclosure but these are on a case-by-case basis. United Kingdom courts rely extensively on this duty of confidentiality coupled with the Human Rights Act 1998 in making decisions on breaches of confidence.

The Duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals

4.4.1. Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4.5. Using and Disclosing Confidential Patient Information

To ensure fair, lawful and transparent processing, privacy notices are available on the Spectrum website, and must be visible at all Spectrum sites, informing patients about:

- The use and disclosure of the information associated with their healthcare
- The choices that they have and the implications of choosing to limit how information may be used or shared
- Their rights in relation to their personal data.

It is extremely important that patients are made aware of information sharing that must take place in order to provide them with high quality care. Whilst patients may understand that information needs to be shared between healthcare professionals, they may not be aware of sharing between different organisations involved in the provision of their healthcare. Efforts must be made to inform them of everyone who will be sharing their information. This is particularly important where disclosure extends to non-NHS bodies. Equally, clinical governance and clinical audits, which are wholly proper components of healthcare provision, might not be obvious to patients and use of information in this way should be drawn to their attention.

Patients have the right to object to the use and disclosure of their confidential information and need to be made aware of this right. Patients need to be made aware that by not consenting to certain disclosures they may be compromising their care. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

4.6. Ethical Standards

The disclosure and use of confidential patient information needs to be both lawful and ethical. The law provides a minimum standard that does not always reflect the appropriate higher ethical standards that the government and the professional regulatory bodies require.

4.7. Protecting Information

It is essential that personal information be effectively protected against improper disclosure at all times. This applies to information held both electronically and on paper. Many improper disclosures are unintentional.

Specific guidance is available through the Information Governance pages of the Intranet. All staff should ensure that the following principles are adhered to:

- All reasonable steps should be taken to ensure that consultations with patients are conducted confidentially;
- Patients' records, either on paper or on screen, should not be left where they can be seen by any unauthorised person;
- Information must be stored securely.
- Identifiable information should not be used in training, testing systems, or demonstrations without explicit consent. Test data should be used for this purpose
- All information held on any portable device or media e.g. laptop computer, memory stick, DVD must be encrypted to Advanced Encryption Standard (AES).

4.8. Physical Security

Access should be restricted to any rooms containing identifiable information. Information should be kept securely within the locked environment when not in use. Never leave personal identifiable information around for others to find.

- Do not walk away from your work area leaving any documents exposed for unauthorised persons to see
- Only have the minimum information necessary on your desk for you to carry out your work. Any other related information should be put away securely
- Do not pass documents containing personal identifiable information to other colleagues by leaving it on a secretary's desk or in an "in" tray. Always ensure that information is in a sealed envelope addressed to the recipient and clearly marked "Confidential"
- Wherever possible, avoid taking confidential information away from your work premises. Where this is necessary in order to carry out your duties (eg, home visits to a patient), you must keep the information securely locked away and make every effort to ensure that it does not get misplaced, lost or stolen. It is acknowledged that it is sometimes appropriate and necessary to leave notes with patients.
- When disposing of paper-based information, ensure that it is disposed of appropriately. Never put confidential information directly into a general waste paper bin or recycling bin
- Working diaries can hold a great deal of personal information and should be kept secure when not in use. Precautions should also be taken when transporting your diary to ensure it is in your care at all times. When you have finished with it or if you leave your job it should be handed in to your line manager who will ensure that it is retained for the appropriate length of time
- If information is no longer required, it should be disposed of appropriately. If information is required for an ongoing purpose, it should be locked securely away

- If documents containing personal identifiable information come into your possession and you are not the intended recipient, you should forward these to the intended recipient. If you identify any document containing personal information, such as letters or results, you should make every effort to decrease the possibility of these being seen by inappropriate persons.

Remember you are bound by the same rules of confidentiality whilst away from your place of work, as you are when you are at your desk. If you are working in a community setting it is understood that relevant information travels with you.

4.9. Physical Transfer of Information

When transferring paper notes, which contain personal identifiable information, make sure "Confidential" is marked in a prominent place on the front of the envelope. Ensure that the address of the recipient is correct and clearly stated, using the following format:

- Full name
- Designation (job title)
- Department
- Organisational address
- Write a return address on the back of the envelope – giving only generic details or PO Box Number
- Where possible patient notes should be hand delivered or collected
- Do not use transit envelopes

Ensure arrangements are in place to check that notes have been safely received e.g. asking the recipient by phone or e-mail that they have received the confidential information

Records should never be left on view in a vehicle. Records must never be left in vehicles overnight.

If you are required to transport records i.e. patient home visits, ensure records are kept securely and not on view. Where several visits are involved, care must be taken to ensure only individual patient notes that are required are taken into that patient's home.

If it is not practicable to return records to base after visits, confidentiality must be maintained within the clinician's home. Records must not be left in vehicles overnight. Records should be returned to base as soon as is practicable.

When transferring electronic and paper-based records in bulk, (in bulk, meaning in excess of 51 records) care must be taken to ensure this is done in a secure way using encryption software and encrypted devices for electronic media approved by Spectrum. For paper records the appropriate NHS courier system should be used. If this is not practicable then secure delivery via the Royal Mail should be considered.

If you are required to send information out of the European Economic Area (EEA) Data Protection requirements within the General Data Protection Regulation places extra requirements on

Spectrum for any transfers of personal information outside of the EEA. If any information is to be transferred, stored or processed outside of the EEA contractual arrangements must be in place. The contract must clearly state that the information will meet the same standards of Data Protection as if it was stored or processed within the EEA. If any member of staff is intending to transfer personal information outside the EEA they must obtain advice from the Caldicott Guardian and the Data Protection Officer. Guidance should be sought to determine if a Data Protection Impact Assessment should be completed.

4.10. Conversations

Ensure you cannot be overheard by unauthorised people when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about confidential information. Do not identify a patient or staff member by name unless it is safe to do so. If personal identifiers are necessary, please remember the following:

Consideration needs to be given to the position of any answerphone to ensure that recorded conversations cannot be overhead or otherwise inappropriately accessed

In clinical areas staff should be aware that other patients in the same room/ward might overhear them. Whilst it is appreciated that it is difficult to manage confidentiality in situations like these, staff are expected to be aware of the possible problems and do all they can to respect the patients' right to confidentiality

It is not appropriate to discuss personal information in public areas eg corridors, stairways, occupied lifts or staff canteen

When speaking to a patient, carer or staff member on the telephone, confirm the caller's identity and ensure they are entitled to the information they are requesting. If in any doubt about the identity of the caller take their telephone number, verify it independently and call them back via the switchboard

Be aware of bogus callers. These can be lone individuals, private investigators or individuals working for debt collection agencies who have been sub-contracted. Extreme vigilance is required at all times. Always verify a caller's details and ensure they are entitled to the information they are requesting before you release it. Alert your line manager if you suspect an instance of a bogus caller.

If you have to leave the phone unattended ensure the hold/mute button on your telephone is activated.

4.11. Sending Personal Information by Fax

Do not routinely send identifiable information by fax. Justify the need to fax the information and anonymise confidential information whenever you can. When sending faxes that contain personal identifiable information try to use a designated Safe Haven fax wherever possible. A designated Safe Haven is a place where a fax containing confidential information can be sent safely in the

knowledge that procedures are in place at the other end to ensure its security. If you cannot access a designated Safe Haven fax machine the following principles should be followed:

- Always use a fax cover sheet, complete with the senders and recipients details
- Telephone first to inform the recipient that you are faxing confidential information
- Ask if they could wait by their fax machine whilst you send the fax
- Ask if they could telephone to acknowledge receipt or contact them after sending
- Always double check that you have keyed in the right number before hitting the "send" key
- Regularly used numbers should be programmed into your fax machine (if possible) to decrease the possibility of keying in the wrong number
- Remove documents immediately from the fax machine once they have been sent
- Do not leave the fax machine unattended whilst faxing confidential information
- If the fax is not collected immediately by the recipient it should be placed in a sealed envelope with their name and 'confidential' written on it
- If you find confidential information left on a fax machine return it in a sealed envelope to the sender. If the sender is unknown, shred the fax
- Never send faxes to destinations where you know they are not going to be seen for some time or outside office opening hours
- Display a poster next to the fax machine to remind users of the above points
- It is advisable to have an audit trail of what has been faxed, by whom and to what location.

4.12. Keeping Computerised Information Safe

The security and confidentiality of information held on computer must be maintained at all times.

- Never leave a computer logged on to a system and unprotected. Always protect the system by pressing Control, Alt & Delete simultaneously on your keyboard and select the option 'lock computer'. This applies no matter how long you are leaving your computer unattended
- Always log off when you have finished. This prevents the risk of unauthorised access to patient information. It also ends the user's session on the computer. Turn off the computer at the end of the working day. If it is necessary to leave it switched on for technical reasons make sure it is locked using Control, Alt & Delete plus option 'lock computer'
- Where it is necessary for personal identifiable information to be stored ensure that it is stored in a secure way with password protection, consideration could be given to restrict access folders if required.
- Never store personal identifiable information on the hard disk of the computer (either on the c-drive or 'my documents'). Seek guidance from the IM&T Manager
- Do not keep any personal identifiable information longer than necessary
- Delete files you do not need to keep and if the information is stored on removable media ensure that it is clearly labelled and locked away.

- Windows users should remember that when deleting files they are moved to the “recycle bin”. Therefore, the recycle bin should be emptied on a regular basis. If in doubt, check with the Service Desk
- Passwords protect both the information and you as a user. Never disclose your password to anyone under any circumstances. Never write your password down and always change your password when prompted. It is recommended that passwords should be a minimum of 8 characters and be a mixture of letters and numbers
- Never use anyone else’s password, login or PIN number. Never, as a manager, ask anyone to use another’s password for convenience. If it is absolutely necessary contact the Service Desk
- If you are issued with a Smartcard you must keep it secure and not permit anybody else to use it. You must not share your PIN or password with any other user. If you lose your Smartcard or suspect it has been stolen or used by a third party you must report the incident to your local Registration Authority as soon as possible via your line manager
- Destruction and/or disposal of computers, or parts thereof, must be carried out by the IM&T Department. Contact the Service Desk for assistance.
- Staff must not store Spectrum information on any type of privately owned computer or storage device
- Always remove your Smartcard when leaving your workstation and it must not be left on display at any time

4.12.1. If You Use a Portable Computer Outside Your Place of Work

Laptops that have identifiable information stored on them must not be taken off the premises unless the information is encrypted

- Do not leave portable computer equipment on view within your car
- Do not leave portable computer equipment in your car overnight
- Store any electronic back-ups securely. Update your information regularly whilst using portable equipment
- Ensure that your computer is password protected
- Ensure that any document, spreadsheets or databases containing confidential or sensitive data are password protected
- All equipment should be locked away when not in use
- Make every effort to ensure that your portable computer does not get misplaced, lost or stolen

Remember, you are bound by the same rules of confidentiality whilst away from your place of work, as you are when you are at your desk.

4.12.2. Use of Removable Data Storage Devices

Removable data storage devices should only be used to transport or store data when other more secure means, such as network shared folders are not available. All such devices must be encrypted to agreed standards.

- Ask the Service Desk for advice as to the most appropriate and secure method
- All removable data storage devices should be stored in a secure environment
- Ensure that data is only held on the removable data storage device for a specific purpose
- As soon as is practicable move the data file(s) back on the secure network
- Ensure that you keep a backup copy of all data files stored on your removable data storage device

4.13. Record Keeping Best Practice

The Records Management Policy has been produced to ensure that Spectrum can control both the quality and quantity of the information that it generates

The Records Management Policy relates to information in any medium, which has been gathered as a result of any NHS activity whether clinical or non-clinical by employees – including external consultants, agency or bank staff.

4.14. Implementation and Dissemination

Following approval by the Data Protection Group and formal ratification from the Finance and Audit Committee, this policy will be disseminated to staff and managers.

As a Spectrum Corporate Policy supporting Data Protection and confidentiality, all staff need to be aware of the key points that the policy covers. The policy will be distributed as a Mandatory Read document, to evidence that all staff have had sight of the document and sign to say that they agree to its contents.

All approved documents will be disseminated to all staff via the intranet and can be cascaded to staff through any of the following methods:

- Team briefings
- One to one meetings / Supervision
- Group supervision
- Practice Development Days
- CPD sessions
- Local Induction

This Policy will be reviewed annually or in line with changes to relevant legislation or national guidance and monitored annually by the Board or Finance and Audit Committee in line with Data Security and Protection Toolkit (DSPT) compliance.

5. Training implications

Document Title:	Data Protection and Confidentiality Policy
Staff groups requiring training:	All Staff

Is the training role specific:	No
Description of training:	E- Learning Induction Specific training where identified following walk rounds, audits and incidents
Existing course available:	Data Security Awareness training Level 1 via either ESR or NHS Digital
Name of training provider:	
Frequency of training:	The level 1 training is required on an annual basis
Length of training:	
Delivery method:	E Learning Face to Face corporate induction and team awareness sessions
Key references / legislation:	General Data Protection Regulation
Location of training records:	ESR

6. Monitoring arrangements

Area for Monitoring	How	Who by	Reported to	Frequency
Risk Management	Spot checks	Compliance Team Information Asset Owners	Data Protection Group	Quarterly
Incidents	Monitoring of incidents reported Trends analysis Frequency Follow up	Head of Compliance	Data Protection Group	Each meeting

Area for Monitoring	How	Who by	Reported to	Frequency
Compliance with training	Monitoring of staff in date with training Requests for additional training			
Complaints				

7. Links to any associated documents

This Policy and Procedure should be read with consideration to the following policies

- Information Sharing Policy
- Pseudonymsation Policy
- Records Management Policy (including Data Retention Guidance)
- Network Security Policy
- Email Policy
- Internet Use Policy
- Mobile Communications Devices Policy

8. References

General Data Protection Regulation 25th May 2018

Data Protection Act 2018

Human Rights Act 1998

9. Appendices

9.1. Information on Caldicott reviews and associated principles.

Caldicott Report and Caldicott 2

The Caldicott Committee, Chaired by Dame Fiona Caldicott, was set up by the Chief Medical Officer for Health following increasing concerns regarding the way information flowed, not only within NHS organisations, but to and from non-NHS organisations also. The resulting report, "The Caldicott Committee: Report on the Review of Patient Identifiable Information" was published in December 1997.

The Report made sixteen recommendations. One of the recommendations was the appointment of a Caldicott Guardian, who should be a senior health professional or an existing member of the management board, for each organisation. The Guardian is responsible for agreeing and reviewing protocols for governing the disclosure of personal identifiable information across organisational boundaries.

The Committee also developed a set of 6 general principles for the safe handling of personal identifiable information and these Principles are the guidelines to which the NHS works. They work hand-in-hand with the Principles of the Data Protection Act 1998. They both cover information held in whatever format – electronic, paper, verbal or visual. The Caldicott Principles must be adhered to when collecting, transferring or generally working with personal identifiable information.

The Information Governance Review, April 2013 (known as **Caldicott 2**), added a 7th Principle:

The Caldicott Principles

i. Justify the purpose for using confidential information
ii. Don't use patient identifiable information unless it is absolutely necessary
iii. Use the minimum necessary patient identifiable information
iv. Access to patient identifiable information should be on a strict need to know basis
v. Everyone should be aware of their responsibilities
vi. Understand and comply with the law
vii. The duty to share information can be as important as the duty to protect patient confidentiality".

The 2013 Review highlights that for health professionals to act in a patient's best interest, they need to have all the available information about the patient to do so. However, it is acknowledged that current information governance provisions (or at least the interpretation of them) have led to information not being shared when it should be. Accordingly, Recommendation 2 of the Review specifically states that:

"for the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual."

Further, the Review also recognises that there are certain situations when sharing of personal information is not just preferable, but vital. An example given of this is within

public health medicine in order to identify people at risk during an outbreak of an infectious disease, or to carry out health improvement and research exercises.

10. Definition of Terms

What is patient identifiable information?

"All items of information which relate to an attribute of an individual should be treated as potentially capable of identifying patients and hence should be appropriately protected to safeguard confidentiality" Caldicott Committee: Report on the review of patient identifiable information, 1997 and The Information Governance Review, April 2013 (known as Caldicott 2) see Appendix 1.

These items include:

Surname	Forename
Initials	Address
Date of Birth	Other dates (eg, death, diagnosis)
Postcode	Occupation
Sex	NHS number
National Insurance Number	Ethnic Group

Local Identifier (eg, hospital or GP Practice Number)

Telephone Number

What is staff identifiable information?

All items of information which relate to staff should be treated as potentially capable of identifying staff and hence should be appropriately protected to safeguard confidentiality.

These items include:

Surname	Forename
Initials	Address
Date of Birth	Occupation
Postcode	NHS or Staff number
Sex	Ethnic Group
National Insurance Number	Telephone number

Salary details

What is Corporate information?

All items of information which relate to the running of Spectrum are classed as corporate information. All such information should be regarded as confidential even if it may be released under the Freedom of Information Act. This includes: -

- Board Papers
- Minutes of meetings

- Details of contracts entered into
- Financial information