Livewell Southwest

Data Protection, Confidentiality, Caldicott and Safe Haven Policy & Procedure

Version No. 1.2

Notice to staff using a paper copy of this guidance

The policies and procedures page of LSW Intranet holds the most recent version of this document and staff must ensure that they are using the most recent guidance.

Author: **Information Governance Group**

Asset Number: **826**

Reader Information

Title	**Data Protection, Confidentiality, Caldicott & Safe Haven Policy & Procedure V.1.2**
Asset number	826
Rights of access	Public
Type of paper	Policy and procedure
Category	Corporate – Information Governance
Subject	Personal Identifiable Information (Corporate & Clinical)
Document purpose/summary	This document describes Livewell Southwest's (LSW's) policy on Data Protection, Caldicott Principles and employees' responsibilities for the safeguarding and sharing of confidential information.
Author	Information Governance Lead
Ratification date and group	24th February 2016. Policy Ratification Group
Publication date	3rd March 2016
Review date and frequency (one, two or three years based on risk assessment)	A full review will take place two years after publication, however it will be monitored regularly and changes made accordingly in line with best practice and legislation.
Disposal date	The Policy Ratification Group will retain an e-signed copy for the database in accordance with the Retention and Disposal Schedule; all previous copies will be destroyed.
Job title	Information Governance Lead
Target audience	All Livewell Southwest staff, contractors and partner organisations working on behalf of LSW that introduce new processes or systems that are likely to involve a new use or significantly change to the way in which personal data is handled.
Circulation	Electronic: (LSW) intranet and website (if applicable) Written: Upon request to the PRG Secretary on ☏ 01752 435104. Please contact the author if you require this document in an alternative format.
Consultation process	Information Governance Group
Equality analysis checklist completed	Yes
References/sources of information	NHS Outer North East London Caldicott Policy (2012) Connecting for Health Information Governance Toolkit (IGT) - https://nww.igt.connectingforhealth.nhs.uk/ (2012) DH: Caldicott Guardian Manual (2010) Confidentiality: NHS Code of Practice (2010) DH: NHS IG - Information Risk Management - Good

	Practice Guide (2009) Mental Capacity Act Code of Practice (2005) Freedom of Information Act 2000 Data Protection Act 1998 Human Rights Act 1998 Access to Health Records 1990 Access to Medical Reports Act 1988 Caldicott Report (1997),
Associated documentation	• Audiovisual Recordings of Patients/Visitors/Staff and Business Activities Policy • Clinical Record & Note Keeping Policy • Communications Systems: Phone, Email, Internet & Fax Policy • Disclosure of Health Records • Freedom of Information & Environmental Information Regulations Guidance • Incident Reporting and Investigation Policy • Information Governance Policy • Information Sharing Policy • IT Security Policy • Privacy Impact Assessment Policy • Records Management Policy • Risk Management Policy • Security Policy • Template for developing Data Sharing Agreements
Supersedes document	New document
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon. PL4 7PY. Tel: 0845 155 8085, Fax: 01752 272522 (LCC Reception).

Document review history

Version no.	Type of change	Date	Originator of change	Description of change
0.1	New document	16/01/13	Information Governance Lead	New document
0.2 to 0.4	New document	07/02/13 & 02/04/13	Information Governance Lead	Inclusion of Mental Capacity Act Code of Practice (2005) & comments from IGG.
1	Ratified	April 2013	Governance & Customer Care Manager	Ratified.
1.1	Amended	July 2014	Governance & Customer Care Manager	White Board information added, section 6.7.2
1.2	Reviewed	December 2015	Internal Audit	2.2 Caldicott Principles Changes to reflect Caldicott 2 and the addition of Principle 7 4.6 Data Owners Now also known as Information Asset Owners / Administrators. 6.6.1 Encrypting Patient Data Inclusion of Datasticks, and reference to fines being up to £500,000

Data Protection, Confidentiality, Caldicott & Safe Haven Policy & Procedure

1 Introduction

1.1 This policy sits within LSW's (LSW) Information Governance Framework, and is concerned with LSW's legal obligation to comply with all appropriate legislation and relevant guidance in respect of Data, Information and IT Security. It covers both information about users of our service and employees.

1.2 Personal information, both corporate and clinically held by LSW is an important and valuable asset. LSW recognises that the safeguarding of personal and sensitive data is crucial, and sharing information between service areas and partner agencies is vital for the provision of co-ordinated and seamless care.

1.3 Legislation does not prevent the sharing of information but places important rules and safeguards that must be observed. The aim of this policy is to describe the roles, responsibilities and principles for ensuring that personal information is handled in a lawful and correct manner.

1.4 This policy applies to all employees working at all levels and grades. It also extends to persons working for LSW such as secondees, agency staff, volunteers, contractors and others employed under a contract of service, and all other individuals using or accessing LSW services and equipment whether on or off site (collectively referred to as staff in this policy).

1.5 Failure of LSW staff to comply with data protection could potentially result in a subsequent investigation by the Information Commissioners Office, with the possible risk of being fined up to £500,000 for very serious breaches.

2. Purpose

2.1 Data Protection Act 1998 (DPA)

2.1.1 This Act applies to all personal identifiable information for all living individuals held in manual files, computer databases, videos and other automated media about living individuals, such as human resources, payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays etc.

2.1.2 The Act dictates that information should only be disclosed on a 'need to know' basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any breach of the DPA with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with LSW policy will be considered a disciplinary offence and may result in serious disciplinary action being taken. Staff could also face criminal proceedings.

2.1.3 LSW has to comply with the principles of good practice known as the eight data protection principles, and we fully endorse these. All staff who process personal information must ensure these principles are followed. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully.
- Be obtained for one or more specified purpose and not be processed in a manner incompatible with that purpose.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary.
- Be processed in accordance with the rights of data subjects under the Act.
- Be kept secure from unauthorised access, unlawful processing, accidental loss or destruction.
- Not be transferred outside the European Economic Area unless that country has an adequate level of protection for data subjects.

2.2 Caldicott principles

2.2.1 The Caldicott Report (1997, reviewed 2013) which provides guidance to the NHS on the use and protection of patient identifiable information formulated seven Caldicott principles for handling patient identifiable information. These are:

- Justify the purpose(s) of using confidential information.
- Only use it when absolutely necessary.
- Use the minimum that is required.
- Access should be on a strict need-to-know basis.
- Everyone must understand his or her responsibilities.
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

2.3 Confidentiality: NHS Code of Practice (2003)

2.3.1 The Code's purpose is to provide guidance to the NHS and NHS related organisations on patient information confidentiality issues. It also considers ways of obtaining and using patient information to comply with data protection legislation, current and planned.

2.4 Supplementary Guidance: Public Interest Disclosures (2010)

2.4.1 This document expands upon the principles set out with the Department of Health's (DH) key guidance Confidentiality: NHS Code of Practice. The document is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest.

2.5 DH Information Security Management: NHS Code of Practice (2007)

2.5.1 This guide refers to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice.

2.6 DH Records Management: NHS Code of Practice (2006)

2.6.1 This guide refers to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England.

2.7 Professional Guidance

2.7.1 As well as an obligation to the organisation, many staff are also bound by the Codes of Conduct of their respective professional bodies and should refer to their respective organisations for details of their guidelines.

2.7.2 Other legislation which makes reference to issues of security and/or confidentiality of personal identifiable information/data are detailed in appendix one.

3 Definitions

3.1 **Personal identifiable information (PID)** is information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual last name or isolated postcode, or small pieces of different information which if taken

together could allow the person to be identified. Examples of personal information are address, data of birth, name etc.

3.2 **Sensitive personal information** is usually treated confidentially and whose loss or misdirection could impact adversely on individuals, the organisation or on the wider community. Sensitive personal information is defined in the DPA where the personal information contains details of:

- Health or physical condition
- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Sexual life
- Criminal convictions

3.3 For this type of information more stringent measures should be employed to ensure that it remains secure and confidential.

3.4 Information about an individual's financial arrangements or specific to an organisation's business operations, finance or security is also likely to be deemed 'sensitive'.

3.5 **Corporate information** is information relating to the business activities of the organisation and in particular, information relating to funding and contracts.

3.6 The term **Safe Haven** is used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post, email, telephone or other means. Any members of staff handling confidential information must adhere to the Safe Haven principles. Safe Haven procedures are set out in point six.

3.7 **Primary uses** are when information is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.

3.8 **Secondary uses** are for non-healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When PID is

used for secondary use this should, where appropriate, be limited and de-identified so that the secondary uses process is confidential.

4 Duties & Responsibilities

4.1 The **Chief Executive** has overall responsibility for the strategic direction and operational management, including ensuring that LSW process documents comply with all legal, statutory and good practice guidance requirements.

4.2 The **Senior Information Risk Officer (SIRO)** is responsible to the Board for ensuring information risk policy is developed, implemented, reviewed and its effect monitored. Privacy Impact Assessment (PIA) is one element of the management of information risk. Information risks needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

4.3 **Caldicott Guardians** were introduced in 1997 following concerns about the use of patient identifiable information in health agencies. Caldicott Guardians have responsibility to ensure that patient identifiable information is safeguarded. The Caldicott Guardian [LSW Medical Director] acts as a conscience in matters of data confidentiality and information sharing. They work as part of a broader Information Governance function, and their key responsibilities are:

- To develop knowledge of confidentiality and data protection matters including links with external sources of advice and guidance.
- To ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- To oversee all arrangements, protocols and procedures where confidential information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.
- To support Information Governance in the development of information sharing protocols.
- To offer support and advice as required to the Information Governance Group on matters relating to confidentiality and patient information.
- Make the final decision in issues that arise regarding the protection and use of personal information.
- In relation to information disclosures, the advice of the Caldicott Guardian should be sought prior to making any statutory or public interest disclosure.

The Caldicott Guardian work plan is attached as appendix two.

4.4 The **Information Governance Group (IGG)** was established in January 2011 to ensure that the Information Governance Framework is progressed. The Framework sets out and promotes a culture of good practice around the processing of information and use of information systems that supports the provision of high quality care to users of our services. The IGG is responsible for:

- Ensuring the organisation has effective policies and management arrangements covering all aspects of Information Governance.
- Ensuring that LSW undertakes or commissions annual assessments and audits of its Information Governance arrangements.
- Produce an annual return based on the Information Governance Toolkit which is signed off by the Board.
- Establish an annual Information Governance improvement **plan**, secure the necessary implementation resources, and monitor the implementation of that plan.

4.5 The **Information Governance Lead** monitors and evaluates the organisation compliance with Information Governance standards as directed by the DH.

4.6 **Information Asset Owners** are responsible for key sets of information held manually and electronically. A register of Information Asset owners is held centrally by the Information Governance Lead. Information Asset Owners will:

- Complete a privacy impact assessment on initiation
- Conduct three monthly information risk assessment on each asset. Updating the corporate risk register if required.
- Control access to the file set / information.
- Make sure that the file set complies with the Safe Haven procedures.
- Identify all personal data held within that file set.
- Inform the IGG of any changes in the processing of personal information.
- Identify and justify how the file set may be used in accordance with the Caldicott principles.

4.7 **All managers** will:

- Ensure that all current and future staff are instructed in their duty of confidentiality and security responsibilities.
- Disseminate to all staff the guidance for obtaining, using and disclosing personal information.
- Ensure that no unauthorised staff or other persons are allowed access to any of the LSW's computer systems or manually held information.

- Determine which individuals are to be given access to specific computer or manual systems. The level of access to specific systems should be on a job function need, independent of status.
- Ensure that relevant system managers are advised about staff changes affecting computer access (e.g. job function changes, leaving a department or the organisation) in order that passwords may be disabled.

4.8 All **staff** are responsible for ensuring they are aware of the Information Governance requirements and ensuring they comply with these on a day to day basis.

5. Procedures

5.1 LSW will only collect information that is necessary to carry out operational needs or to comply with legal requirements.

5.2 When collecting service user data, service areas will ensure that individuals are adequately informed about the uses of their information. See appendix three for LSW's Privacy Notice.

5.3 In some cases LSW may only process personal information with the explicit consent of the subject.

5.4 Retention of personal information

5.4.1 LSW will set retention periods for all personal information falling within the remit of the DPA. Health records & Corporate records will be retained and disposed of in accordance with NHS Records Management Code of Practice. Please refer to the Records Management Policy available on the intranet.

5.5 Access to personal information

5.5.1 Data subjects are entitled to a copy of personal information held about them (Subject Access), providing that the information falls within the remit of the DPA. Please refer to the Disclosure of Health Records available on the intranet.

6 Requirements for safe havens

6.1 We hold large amounts of confidential information about our service users and staff. **Staff must ensure that they have done everything possible to protect this information,** and comply with the Caldicott, Data Protection principles.

6.2 Communication by post

6.2.1 Internal post

- This is considered secure and can be used for personal information as long as multiple letters/documents are contained in sealed and secure envelopes/bags, so that they cannot simply fall out.
- Health records or other confidential information for transportation between sites/departments must be enclosed in sealed bags/envelopes and labelled appropriately i.e. 'Confidential', and if relevant marked 'to be opened by addressee only'. The senders address must be clear on the reverse. Guidelines for the transporting of health records are available on the intranet, and from the Health and Corporate Records Team on LSWcic.hrt@nhs.net.

6.2.2 External post

- Written communications containing sensitive/personal information (e.g. referral letters, appointment letters and test results) should be transferred in a sealed envelope, addressed to a named recipient and clearly marked 'Private and Confidential'.
- Constant care must be taken to ensure that only the correct documents are placed inside the envelope. Confidentiality breaches often occur when more than one patient's correspondence is placed into an envelope.
- Always check that address details are correct by confirming them with the destination and always include the post code, even when using the internal mail service.
- If appropriate, a designated person should be informed that the information has been sent and arrangements made within their location to ensure that the envelope is received within the expected timescales.
- For situations where proof of posting and confirmation of receipt are required, either a Recorded Delivery or Special Delivery service should be used.

6.3 Verbal communication

- A considerable amount of information sharing takes place verbally, often on an informal basis, and care should be taken to ensure that confidentiality is maintained in such discussions.
- If information is to be shared by phone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant phone number, double checking that it is the correct number for that individual / organisation and then calling the recipient

back. Ensure no information is disclosed from LSW and that the persons whose identity is being validated provides the information.

- Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard by other staff who do not have a 'need to know'.
- Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts etc.
- Messages containing personal information should not be left on answer machines unless a password is required to access them. They should also not be stored on communal systems.

6.4 Communication by fax machines

6.4.1 One of the most common breaches of confidentiality occurs when documents that contain patient identifiable information are sent by fax machine. Many fax machines are in corridors or open plan offices and are used by several different departments. People come and go collecting faxes but do not always check that all the pages belong to them; this increases the risk of information being seen by unauthorised persons. **Secure email is always the preferred option and fax should be the last resort where email is not possible**

6.4.2 If faxing is essential the risk should be minimised. Many NHS provider organisations have designated fax machines as 'Safe Haven' machines. These are located in a secure area and are used to receive documents of a private and confidential nature. Staff should:

- Telephone the recipient of the fax let them know that you are about to send a fax containing confidential information.
- Ask if they will wait by the fax machine whilst you send the document.
- Ask if they will acknowledge the receipt of the fax.
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential.
- Check the fax number you have dialled and check again that it is correct before sending.
- Request a report sheet to confirm that the transmission was received.

6.4.3 Further guidance and a fax cover sheet are available in the Communications Systems: Phone, Email, Internet & Fax Policy available on the intranet.

6.5 Transporting paper documents

- When transporting records/documents between separate LSW sites this must be done using the official internal postal system, the records

must be transported in sealed transport envelopes or transport bags/boxes. The sender and the recipients address must both be on the envelope. Guidelines for the transporting of health records, including the use of taxis, is available on the intranet, and from the Health and Corporate Records Team on LSWcic.hrt@nhs.net

6.6 Computers and electronic storage devices

- 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 should be locked or switched off when you are away from your desk for any length of time.
- Information should be held on the organisation's network servers, not stored on local hard drives.
- All person identifiable information sent by email must be sent from one NHSmail address to another secure email domain such as NHS.net to NHS.net or via an encrypted attachment.
- It is now possible to securely exchange sensitive information from NHSmail with users of non-accredited secure email services, those ending in @nhs.uk or Hotmail, Gmail and Yahoo for example. This replaces the SecureSend facility we previously advised Trust staff to use. Details on how to so this is on the PICTS portal, under help and guidance 'Sending confidential and patient identifiable information from NHSmail.
- In the rare event where a situation arises where it is not possible, a risk assessment should be undertaken by the Caldicott Guardian in conjunction with the partners, and the attachment encrypted.

6.6.1 Encrypting Patient Data on CDs and DVDs

- Patient identifiable data should never be written to Datasticks, CDs or DVDs without encryption. A number of organisations have been fined by the Information Commissioner when staff have failed to do this, with fines potentially totaling £500,000 (See ICO Website). Further information and guidance on how to secure data can be found on the PICTS Portal: http://nww.plymouthict.nhs.uk/Home/tabid/55/Article/365/encrypting-patient-data-on-cds-and-dvds.aspx, and guidance regarding confidential data exchange via email is set out in the Communications Systems: Phone, Email, Internet & Fax Policy available on the intranet.

6.7 Whiteboards/Notice boards

6.7.1 Whiteboards that are placed in areas accessed by the public (wards, treatment rooms etc.) should only contain sufficient detail to locate the patient, so as not to disclose patient related confidential information.

6.7.2 Displaying Personal Information (for example on white-boards)

Boards containing patient information/person identifiable information should ideally be sited in areas that are **not** generally accessible by the public, e.g. staff offices. These rooms should be:

- Clearly marked 'staff only' and windows obscured appropriately.
- Where the organisation has assessed that repositioning is impractical, the boards should contain only sufficient detail to locate the patient and they must not contain confidential information.
- White boards in patient areas should only state the patient's first initial and surname (both initials preferably), and if a patient insists that they do not want this information displayed in a visible public area their decision must be respected.
- No other patient identifiable information should be put onto whiteboards located in general public areas, for example address, date of birth or specific clinical details.
- If it is absolutely necessary to put clinical information onto a whiteboard, the information should be abbreviated or symbolised so that only health professionals can understand the information and not other members of staff that may come into the department.
- The use of personal information in patient areas should be carefully considered and a risk assessment undertaken by an appropriate manager.

6.8 Physical location and security

If confidential information is received to a specific location:

- It should be to a room/area that is lockable or accessible via a coded key pad known only to authorised staff.
- The room/area should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to all members of staff working in the same building or office, or to visitors.

- The room/area should conform to health and safety requirements in terms of fire, flood, theft or environmental damage.

7. Pseudonymisation

7.1 A fundamental principle of the Data Protection Act 1998 is to use the minimum personal data to satisfy a purpose and to strip out information relating to a data subject that is not necessary for the particular processing being undertaken.

7.2 Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. This allows patient linking analysis needed within secondary uses. Pseudonymisation is a core element of Secondary Uses Services (SUS) and should be applied across LSW.

7.3 All business processes within LSW must be documented. Business processes can include, but are not limited to:

- The process of using patient data for primary uses (appointment bookings, management of waiting lists etc.)
- The process for using patient data for secondary uses.
- The use of Patient Identifiable Data (PID) for a combination of primary and secondary.

7.4 De-Identification

7.4.1 Staff only have access to the data that is necessary for the completion of the business activity which they are involved in. By de-identification users are able to make use of patient data for a range of secondary purposes without having to access the identifiable data items. The aim of de-identification is to obscure the identifier data items within the patient records sufficiently that the risk of potential identification of the subject of a patient record is minimised to acceptable levels, this will provide effective anonymisation. Although the risk of identification can not be fully removed this can be minimised with the use of multiple pseudonyms.

7.4.2 De-identification can be achieved by:

- Removing patient identifiers.
- The use of the identifier for example; value ranges instead of age.
- By using a pseudonym.

7.4.3 To effectively pseudonymise data the following actions must be taken:

- Each field of PID must have a unique pseudonym.
- Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability e.g. in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers.
- Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports.
- Pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised.
- The secondary use output must only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines.
- Pseudonymised data should have the same security as PID.

8. Confidentiality audit approach

8.1 With advances in the electronic management of health and employment information, the requirement to monitor access to such confidential information has become increasingly important.

8.2 With more staff using electronic systems, it is imperative that access is strictly monitored and controlled. The movement of confidential information via these methods poses the threat of information falling into the hands of individuals who do not have a legitimate right of access to it.

8.3 Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented may result in a breach of that confidentiality, therefore contravening the requirements of Caldicott, the Data Protection Act 1998, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

8.4 The SIRO will ensure that audits of security and access arrangements within each area are conducted on a regular basis. Audits should include:

- Failed attempts to access confidential information.
- Repeated attempts to access confidential information.
- Access of confidential information by unauthorised persons.
- Evidence of shared login sessions/passwords.
- Staff awareness of LSW policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to

confidentiality.

- Appropriate use of smartcards.
- Appropriate allocation of access rights to systems which contain confidential information.
- Appropriate staff access to physical areas.
- Storage of and access to filed hard copy patient notes and information.
- Security of confidential fax handling.
- Confidential information sent or received via e-mail, security applied and e-mail system used.
- Information removed from the workplace - has authorisation been gained either for long-term or short term removal?
- Security applied to laptops and portable electronic media.
- Evidence of secure waste disposal.
- Use of whiteboards for confidential information.
- Information flows of confidential information.
- Appropriate transfer and sharing arrangements are in place.
- Security and arrangements for recording access applied to manual files both live and archive e.g. storage in locked cabinets/locked rooms.

8.5 Confidentiality audits can be carried out in a number of ways:

- Interviews with staff using structured questionnaires.
- Notified audit visits with structured questionnaires.
- Spot checks at random work areas.
- Audit carried out by the Data Owners on electronic records.
- Registration Authority (smartcard usage) enhanced reporting facilities
- As part of an investigation into a potential breach of confidentiality/data loss
- Investigation of reports/Caldicott log.
- Monitoring of reported incidents.

8.6 Confidentiality Audit results will be collected on a standard template and recorded for analysis and future reporting. Reporting will be to the Information Governance Group and will highlight any areas for improvement and learning.

8.7 If a breach or any risks of breaches in person-identifiable confidential information are identified from the audits, matters will be reported and investigated through the LSW's Incident Reporting Procedure and Disciplinary Policy if appropriate.

8.8 The Information Governance Group is tasked with developing an annual confidentiality audit plan, and will identify appropriate staff to undertake these audits.

9. Sharing information with other organisations

9.1 Staff sharing personal information with other agencies should be aware of data sharing agreements between LSW and those agencies. Data sharing agreements provide assurance that these agencies are able to comply with the safe haven ethos and meet legislative and related guidance requirements. Further guidance is set out in appendix five.

9.2 Data sharing agreements are published on the intranet, or alternatively you can contact the Information Governance Lead on LSWCIC.InformationGovernance@nhs.net who can provide a list.

10 Training Implications

10.1 All new staff and existing staff will be made aware of this policy via the induction process and at annual mandatory training. A copy will be available on the intranet. Managers must highlight to staff their responsibility to ensure that they have sight of the content of this policy and the importance that LSW places on this matter and remind staff of the Information Governance clauses contained in their staff contract.

11 Monitoring Compliance and Effectiveness

11.1 All breaches of this policy should be reported in line with LSW Incident Reporting and Investigation policy.

11.2 On a routine basis a report on breaches of this policy shall be presented to the Information Governance Group. The information will enable the monitoring of compliance and improvements to be made to the policy. It will also be monitored through the annual submission of the Information Governance Toolkit.

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice, Safety & Quality

Date: 1st March 2016

Appendix One: Legislation relating to personal identifiable information

Access to Health Records Act 1990: The Act provides controls on the management and disclosure of health records for **deceased** patients. Thus the personal representative of the deceased or a person who might have a claim arising from the patient's death can apply to gain access to the files.

Access to Medical Reports Act 1988: This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Human Rights Act 1998: Article Act of the Act covers an individual's right to privacy and a service user's right to expect confidentiality of their information at all times. It provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. Each organisation must act in a way consistent with these requirements. It must take individuals rights into account when sharing personal information about them.

Freedom of Information Act 2000 (FOI): The FOI Act came into force in November 2000 and gives individuals rights of access to recorded information held by public authorities subject to certain exemptions and conditions.

Regulation of Investigatory Powers Act 2000: This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Common Law Duty of Confidentiality: The Duty prohibits use and disclosure of information, provided in confidence unless there is a statutory or court order requirement to do so. Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure.

Computer Misuse Act 1990: This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access.

Crime and Disorder Act 1998: The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information.

Appendix Two: Caldicott Guardian work plan

The Caldicott Guardian will oversee the annual work plan.

Policy and Procedure Development

- The Caldicott Guardian should be an integral part of an Information Governance Group which promotes a unified approach to Information Governance and which supports the development of an IG infrastructure. Part of this would involve approval and reviewing of policies and procedures relating to Data Protection and Confidentiality.

Information Life Cycle and Records Management Procedures

- The Caldicott Guardian must be consulted by the Health & Corporate Records Manager to ensure that the organisation's Records Management policy and implementation programme is adhering to the DH guidance and protocols on confidentiality (IGT13-400).

Information Security

- The Caldicott Guardian will be briefed and updated by the Information Security Manager to ensure that security risks to person identifiable and confidential patient information are reported and addressed (IGT10-301).
- The Caldicott Guardian will monitor incident reports indicating loss of confidential information.
- Stolen computers/laptops and will have responsibility for investigating the any breach of confidentiality (IGT13-206).

Contractual Information Governance

- The Caldicott Guardian must sign an Information Sharing Protocol outlining rules relating to the sharing of information with other organisations and provides guidance to staff in relation to sharing confidential information. (IGT13-207)

Data flow mapping

- The Caldicott Guardian will oversee and approve the annual data flow mapping process.

Appendix Three: Privacy Notice

LSW ("We" or “LSW”) are committed to protecting and respecting your privacy. This notice (and any other documents referred to in it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our practices regarding your personal data and how we will deal with it, including:

- What personal identifiable information of yours is collected.
- What organisation is collecting the information.
- How the information is used.
- With whom the information may be shared.
- What choices are available to you regarding collection, use and distribution of the information.
- What kind of security procedures are in place to protect the loss, misuse or alteration of information under our control.
- How you can correct any inaccuracies in the information.

This notice only applies to how we process personal data. For the purpose of the Data Protection Act 1998 (the **Act**), the data controller is LSW CIC (Notification Number Z2807096), a community interest company registered under company number 07584107 of Local Care Centre, 200 Mount Gould Road, Plymouth, Devon, PL4 7PY.

Information we may collect from you

During the course of our activities, we may collect and process the following data about you:

- We will collect store and process personal information about our patients and staff. All personal and personal health information obtained about patients or staff is treated as confidential, along with all corporate information.
- Through the provision of our healthcare services, including: inpatient rehabilitation and intermediate care; mental health and learning disability services; community services; and children and young people’s services.
- Through research, whether market or clinical (we may ask you to complete surveys that we use for research purposes, although you do not have to respond to them).
- Details of current, past and prospective employees.
- If you are suppliers, or others that we communicate with.
- If you contact us, we may keep a record of that correspondence.
- Through CCTV monitoring at our premises.

Uses made of the information

We use information held about you in the following ways:

- To allow us to provide health services and to carry out our obligations to you.
- To notify your general practitioner or social / welfare advisors.
- Anonymised finding from our research.
- For education and training.
- To notify you about changes to our service.
- To enable us to comply with our obligations under the any relevant legislation.
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation or to protect the rights, property, or safety of LSW CIC, our patients, or others.
- We will not disclose your details to anybody outside of the NHS without your permission, unless we have a lawful reason to do so, for example disclosure is necessary for crime prevention or safeguarding purposes. We also undertake to only hold your information for as long as is necessary for providing a service to you.

Access to information

The Act gives you the right to access information held about you by making a Subject Access Request (as described in the Act). You can do this by writing to the Data Protection Officer, Hatfield House, Plymouth. Tel: 01752 434525

Appendix Four: Return address protocol for Mental Health Services

LSW sends out patient sensitive information via the postal service on a daily basis, whilst all measures are taken to ensure the postal address is correct, errors do occur and patient's details are not always correct on the information systems. With this in mind it is necessary to instigate a process whereby any undeliverable post is returned to LSW, without the confidentiality of the patient being breached.

A further issue has been brought to the attention of LSW following a complaint regarding a return address label identifying the services, which the post originated from. It can be appreciated those patients who are receiving correspondence from the Mental Health Services, may not wish it to be known to other persons who may for example share the same postal address.

The purpose of this guidance is to identify a system by which patient sensitive correspondence can be returned to LSW in a way that does not identify the sender as being a mental health service.

The majority of our services do not have a mental health service identifiable name, and for these it is proposed to use the postal address only.

Three proposed systems have been devised to take into account the name of units/services and the type of accommodation occupied, and are as follows:

1) **Full Postal Address** – for those units/services which are stand alone/single users of an address which is not identifiable as a Mental Health Service, i.e. Syrena House would be LSW, Syrena House, 284 Dean Cross Road, Plymstock, Plymouth, PL9 7AZ.

2) **Partial Postal Address** – for those services with a Mental Health Service identifiable name or address, who are the sole users of a building, it is proposed to use LSW and post code i.e. Glenbourne Unit would be LSW, Plymouth, PL6 AF.

3) **Team Identifiable System** – for those buildings which accommodate more than one service/team, it will be necessary for the services/teams involved to identify a means to ensure the return mail is returned to the correct team, ensuring patient confidentiality is not breached. Each team would need to be allocated a letter, e.g. Team A, Team B, and the full postal address ensuring that no Mental Health Service identifiable information was used, i.e. Assertive Outreach Services would be Team A, LSW, Riverview, Mount Gould Hospital, Mount Gould Road, Plymouth, PL4 7QD and Home treatment Team would be Team B at the same address.

It is essential that all teams occupying the same building reach an agreement on a central delivery point for the return mail, which can then be passed on to the correct team, i.e. all mail will be returned to Glenbourne reception who will have the list of teams and will place in appropriate pigeon hole.

It is proposed the following units/services use the full postal address system:

- Syrena House
- Gables
- Community Forensic team
- 140 Mount Gould Road
- Elmview, Plympton Hospital (do not use **Mental Health Centre)Needs to be Plympton Clinic**
- Edgecombe Ward
- Greenfields Ward
- Insight Team

The following units/services will use the partial address system:

- Lee Mill Unit (NB: must stipulate LSW as 2 properties share same postcode).

The following units/services to team identifiable system with full address:

- Avon House
- Riverview
- Westbourne Unit

The following units/services to Team Identifiable system with partial address address:

- Glenbourne Unit

As an additional security measure, the return address labels should be placed over the sealed edged of envelope to prevent tampering.

Appendix Five: Data Sharing Agreements

1. What are Data Sharing Agreements?

These tend to be known as many things including; Information Sharing Protocols, Data Exchange Agreements, Information Access Agreements and the list goes on. In essence they should be seen as a document that outlines the following to ensure the process is legal:

- Who is involved in the process.
- Why is the sharing taking place.
- What is being shared .
- Which secure method of transfer will be used.
- When will the transfers take place (daily, weekly etc.).
- How individuals will be informed about the use of their information.
- Monitoring and incident management processes.

2. Do you need a Data Sharing Agreement?

If you are sharing individual elements of information on a one off, or non-routine basis, then you do not need a DSA but staff must follow the guidance set out in this policy so that information is transferred securely.

If you are making more routine transfers of information, or lots of records at a time then it would be advisable to document what is involved.

Is it a legal requirement to have a Data Sharing Agreement? Legally no, however organisations must be assured that the use and disclosure of information is informed, secure and limited to what is required. Data Sharing Agreements can be used to document and monitor this to ensure compliance from the outset.

3. Data Sharing Agreements (Tiers)

As Data Sharing Agreements have developed over time they tend to follow a tiered model, namely:

Tier One	**Overarching Data Sharing Agreement**: This is a high level agreement to share information within the limits of law and guidance e.g. where the organisation has indicated that it is willing to enter into information sharing agreements with partners, where appropriate. This document is signed by the Chief Executive of participating organisations, or equivalent.
Tier Two	**Data Sharing Arrangement**: This sits under the Tier One and outlines the parameters for sharing, what is to be shared, the purposes and legal basis for sharing. This document is agreed and signed by the Caldicott Guardian in an NHS provider organisation.
Tier Three	**Operational Arrangement**: This sits under the Tier Two and describes the day to day operational processes that ensure the sharing is carried out to good governance standards.

LSW is likely to develop specific agreements in relation to tiers two and three.

4. Template for Data Sharing Agreements

Depending on the nature of the information to be shared and who with, Data Sharing Agreements will differ in length and contents. A template for developing Data Sharing Agreements is available on the intranet to assist staff with the creation of agreements.