Livewell Southwest

Information Technology Security Policy

Version No 9.2
Review: April 2017

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 Lead & Plymouth Information Communication Technology Service (PICTS)**
Asset Number:	**174**

Reader Information

Title	**Information Technology Security Policy V9.2**
Asset Number	174
Rights of Access	Public
Type of paper	Policy
Category	Non-Clinical
Document Purpose and Description	This policy defines information security protocols, procedures and controls to protect to a consistently high standard, all information assets held on and processed by the organisation's systems, staff and contractors, from internal or external damage, either deliberately or accidentally
Author	Claire Batten, Head of Information Governance & Records Management (Incl. Policies)
Ratification Date and Group	19th March 2014, Policy Ratification Group. (Updated April 2017. For ratification at May 2017 PRG)
Publication Date	20th April 2017
Review Date and Frequency of Review	Three years after publication, or earlier if there is a change in evidence
Disposal Date	The Policy Ratification Group will retain an e-signed copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or withdrawn from circulation
Job Title of Person Responsible for Review	Claire Batten, Head of Information Governance & Records Management (Incl. Policies)
Target Audience	All Livewell Southwest staff
Circulation List	Electronic: Plymouth Intranet and LSW website Written: Upon request to the Policy Ratification Secretary on□ 01752 435104 Please note if this document is needed in other formats or languages please ask the document author to arrange this
Consultation Process	Information Governance Group
Equality Analysis Checklist completed	Yes
References/Source	• Copyright, Designs and Patents Act (1988) • The Computer Misuse Act (1990) • The Data Protection Act (1998) • Human Rights Act (1998) • Regulation of Investigatory Powers Act (2000) • Freedom of Information Act (2000) • Confidentiality: NHS Code of Practice (2003)

	• DH: NHS IG - Information Risk Management - Good Practice Guide (2009) • Health and Social Care Act (2012) • DH: NHS Information Governance Toolkit V.11 • The Common Law Obligation of Confidentiality • DH: Information: To Share or Not to Share? The Information Governance Review (2013)
Associated Documentation	• Business Continuity & Service Recovery Policy • Communications Systems: Phone, Email, Internet & Fax Policy • Data Protection, Confidentiality, Caldicott and Safe Haven Policy • Incident Reporting and Investigation Policy • Information Governance Policy • Information Sharing Policy • Privacy Impact Assessment Policy • Risk Management Policy • White Board info
Supersedes Document	Information Technology Security Policy V9.1
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
For previous review history please contact the PRG secretary.				
8.1	Update	January 2010	Policy Ratification Secretary	Add letter from Chief Information
8.2	Reviewed	March 2011	Author	Reviewed, no changes made.
8.3	Extension	March 2013	A Saxby	Extended, no changes made.
8.3	Extension	September 2013	A Saxby	Extended, no changes made.
9	Full Review	January 2014	Information Governance Lead	Adopted guidance from PICTS who provide LSW Information Technology (IT) security and IT monitoring.
9.1	Extended	May 2016	Information Governance, Records, Policies & Data Protection Lead.	Formatted to LSW and Extended
9.2	Full Review	April 2017	Head of IG & Records Management	Added section on Network Drives

Information Technology Security Policy

1. Introduction

1.1 Livewell Southwest (LSW) acknowledges that information is a valuable asset; therefore it is in its interest to ensure that the information it holds, in whatever form, is appropriately protected in the interest of all its stakeholders.

1.2 It is therefore of paramount importance to ensure that information is managed and that appropriate policies, procedures, management accountability and structures are in place to provide a robust governance framework for information management.

1.3 Livewell Southwest is under an obligation to both staff and patients to ensure that their personal information is:

- Recorded accurately.
- Not modified or lost during storage or transfer.
- Not disclosed to unauthorised individuals.
- Made available when and where needed for its intended purpose.
- Not processed for any other purpose other than intended without consent.

1.4 The organisation also depends on information systems for its business viability, for example, contract monitoring, financial, personnel, supplies and many department systems. The correct functioning of all these systems is critical to the efficient running of the organisation.

2. Purpose of this policy

2.1 The purpose of this Information Security Policy is to maintain:

Confidentiality Access to data must be kept to those with specific authority to view the data.

Integrity Information is to be complete and accurate. All information systems, assets and networks must operate correctly.

Availability Information must be available and delivered to the right person, at the time when it is needed.

2.2 It will establish and maintain the security and confidentiality of information assets, information systems, applications and networks.

3 Definitions

3.1 Information System

An information system is a combination of hardware, software, set up and trained personnel organised to help planning, control, coordination and decision making in an organisation.

3.2 Information Asset

An information asset is a body of information that has value to the organisation, its business operations and its continuity. Plymouth Information and Communication Technology Service (PICTS) maintain an Information Asset Register for LSW which is reviewed annually for accuracy and completeness.

3.3 Information Asset Owner

Information Asset Owners (IAO) are senior individuals who provide assurance that information risk is being managed effectively in respect of the information assets they ‘own’.

3.4 Information Asset Administrator

Information Asset Administrators (IAA) are System Managers who are familiar with the information asset within their area. They ensure that policies and procedures are followed and recognise actual or potential security incidents of the asset.

4 Duties and Responsibilities

4.1 LSW Board

- It is the role of LSW Board to define the organisation’s policy in respect of IG and meeting legal, statutory and NHS requirements.
- LSW has appointed a Senior Information Risk Owner (SIRO) at Board level who has clearly defined Board level responsibility for overseeing all the diverse aspects of IG, information risk and information security within LSW. The SIRO is the Director of Finance & Deputy Chief Executive.

4.2 Senior Information Risk Owner (SIRO)

- The SIRO is responsible for and takes ownership of the organisation’s IG/risk policy and acts as advocate for Information Governance (IG) risk on the Board.
- Authorises the Department of Health (DH) IG Toolkit self-assessment submissions and ensures that an effective information assurance

governance infrastructure is in place. This includes information asset ownership, reporting, defined roles and responsibilities.

4.3 Caldicott Guardian

- The Caldicott Guardian acts in a strategic and advisory capacity in the use and sharing of patient information.
- Responsible for approving, monitoring and reviewing protocols governing access to person identifiable information by staff within LSW and other organisations both NHS and non NHS.
- This role is undertaken by the Medical Director.

4.4 Information Governance Group

- Responsible for ensuring there is a robust IG management framework to support the current and evolving IG agenda within LSW.
- This includes monitoring compliance of the DH IG Toolkit, developing and maintaining policies, standard procedures and guidance, raising awareness of IG across the organisation.
- Reports by exception to LSW Safety, Quality & Performance Committee on IG issues and IG risk.

4.5 Information Governance Lead

- Responsible for leading the work of the Information Governance Group, co-ordinating the various strands into a comprehensive work programme to ensure LSW meets its statutory and regulatory obligations.
- Supports the SIRO and Caldicott Guardian in the IG agenda, provides advice and guidance to LSW on matters relating to IG and responsible for the timely completion and submission of the end of financial year DH IG Toolkit self-assessment.

4.6 Information and Communication Technology (ICT) Security Coordinator

- Responsible for coordinating information technology security for LSW.

4.7 Managers

- Responsible for ensuring that IG policies, procedures, standards and guidelines are built into local processes and that there is on-going compliance.

4.8 All staff

- All staff, whether permanent, temporary or contracted, including students, contractors and volunteers shall comply with LSW IG policies and procedures to ensure that no breach of information security or confidentiality result from their actions.

4.9 Third party contractors/third parties

- Appropriate contracts and confidentiality information security agreements shall be in place with third party contractors/third parties where potential or actual access to information assets is identified.

5 Access Controls

5.1 PICTS are responsible for providing LSW's IT Security.

5.2 Staff are required to complete the PICTS Registration Authority process to receive a network account. Individual registration processes may exist for other information assets and systems.

5.3 Only authorised staff and third party contractors will be provided with access to information assets and information systems. Information Asset Owners will hold separate policies and registration processes where required and be responsible for ensuring authorised personnel have access only to areas appropriate to their business need. These policies will be defined in LSW System Level Security Policies for that particular information system.

5.4 Passwords are required to be strong as the system permits and ideally consist of eight or more characters, at least one numeric or special character. The information system should enforce password changes every 60-90 days.

5.5 Third party contractors, suppliers or volunteers who have a business need to access information systems and assets are required to have an honorary contract with LSW or have applied for third party access in accordance with PICTS.

6 Electronic Software

6.1 Only software approved by PICTS may be installed on LSW systems. Software purchased by LSW remains the property of LSW even when not installed and should never be transferred to non-LSW devices without prior written approval and transfer of license(s).

6.2 PICTS are responsible for maintaining an effective compliance position in respects of software licensing. Where software is installed without a valid license it may be removed. PICTS will conduct regular software audits and usage will be monitored and metered to help in identifying software which is not in use and can be recovered for redistribution.

7 Equipment Security

7.1 In order to minimise loss or damage to all assets, equipment will be physically protected from security threats and environmental hazards, based on risk assessments by the IAA (System Manager).

7.2 Equipment assigned to individuals (e.g. laptop and/or a mobile telephone) is the personal responsibility of that individual and all relevant precautions should be taken to ensure continued protection from data loss or theft. Please refer to LSW Communications: Phone, Email, Internet and Fax Policy for further details.

7.3 Disposal of electronic information assets must be coordinated through PICTS. Personal devices may not be used for the storage, processing or transmission of business or personal confidential data. Certain removable storage devices defined by PICTS, purchased privately, may be used if they meet security and encryption requirements which are available upon request.

8 Access to Network Services

8.1 Access to network services is restricted to LSW devices or third party systems where prior approval from PICTS has been granted. No personal devices are permitted to access LSW network. An exception to this rule is access provided by the private wireless network ‘WiFi Spark’ where devices are separated from LSW network using appropriate security protocols.

9. Network Drives

9.1 The H: Home Drive should always be used to save information. No information should be stored on the C Drive of any hard drive.

9.2 If you need to share information with colleagues a Group Shared Drive can be created; with one named individual taking ownership for the shared drive. This individual is responsible for ensuring that they regularly review who has access to the information on the drive.

10. Antivirus and Malware Protection

10.1 Antivirus and malware protection is the responsibility of PICTS to configure, maintain and monitor. All LSW devices are required, where possible, to have Sophos antivirus and malware protection software installed. Devices which cannot be joined to the Windows network are required to have alternative precautions configured to protect against viruses and malware.

11. Removable Storage Devices and Media

11.1 All LSW devices where possible will have Sophos Endpoint Control software installed through PICTS and removable storage devices must be encrypted to a specified standard.

11.2 Personal confidential data written to CD or DVD must first be encrypted and PICTS will be able to provide further advice regarding this.

12. Internet, Email and Cloud Storage

12.1 The use of the Internet is defined in the Communications: Phone, Email, Internet and Fax Policy. Use of email is defined in the NHSmail Acceptable Use Policy. Emails containing personal confidential data should be encrypted in transit.

12.2 Under no circumstances should personal confidential data be uploaded to and stored within cloud storage services (e.g. Dropbox, LiveDrive etc.). Use of these services is only allowed for anonymised data or publically available documentation.

13. Assurance

13.1 Each system or collection of information assets which confidential personal data will have a nominated Information Asset Administrator (System Manager) responsible for the creation and on-going review of the System Level Security Policy (SLSP) and accompanying risk assessment. SLSPs will be reviewed annually and form an integral part of the Information Governance Management Framework.

14. Security of Paper Information Assets

14.1 Desks and filing cabinets that contain confidential personal information should be kept locked and the keys secure when not in use. Offices should be locked when unoccupied.

14.2 Paper based assets should either be shredded or disposed of in marked confidential waste bags in line with LSW Safe Handling and Disposal of Healthcare Waste Policy.

15. Business Continuity and Service Recovery

15.1 The organisation will ensure that business continuity and service recovery plans are produced for all critical information, applications, systems and networks. It is the responsibility of Information Asset Administrators (System Managers) to ensure that this is kept up to date, recorded in SLSP and revised annually.

16. Security Incidents

16.1 All security incidents and weaknesses relating to any information asset will be reported and investigated in accordance with LSW Incident Reporting & Investigation Policy.

17. Training Implications

17.1 The LSW Information Governance Group has identified training needs for staff regarding this Policy. Training will be delivered at Corporate Induction and form part of the annual mandatory update for staff. The Information Governance Lead will provide on-going awareness of information security matters via LSW communication networks.

17.2 PICTS will provide training in IT security awareness as required.

18. Monitoring

18.1 Monitoring compliance of this policy will be undertaken by LSW's Information Governance Group and PICTS. Breaches of this policy are to be recorded as incidents using LSW's incident reporting process. PICTS are responsible for the monitoring of any access to the LSW network to establish breaches of the IT Security Policy. PICTS are also responsible for ensuring for that suitable audit tools are in use which enforces policy.

18.2 Compliance with this policy will be monitored by the completion of the IG Toolkit where evidence submitted is audited annually.

18.3 Quarterly IG Toolkit update reports will be presented to the Information Governance Group. The Information Governance Lead will monitor national and local developments that may affect this policy.

All policies are required to be electronically signed by the Lead Director. Proof of the e-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.

Signed: Director of Finance.

Date: 03/04/2016