Lincolnshire Partnership
NHS Foundation Trust

REF: Policy 8B

Lincolnshire Partnership NHS Foundation Trust (LPFT)

Information Management & Security Policy

DOCUMENT VERSION CONTROL	
Document Type and Title:	**Information Management & Security Policy**
Authorised Document Folder:	**IM&T**
New or Replacing:	**Replacing version 7**
Document Reference:	**INF08B**
Version No:	**V8**
Date Policy First Written:	**February 2006**
Date Policy First Implemented:	**March 2006**
Date Policy Last Reviewed and Updated:	**March 2016**
Implementation Date:	**30 October 2017**
Author:	**Cassie Scullion Senior Information Governance Advisor**
Approving Body:	**IM&T Committee**
Approval Date:	**27 October 2017**
Committee, Group or Individual Monitoring the Document	**Information Governance and Records Management Group**
Review Date:	**August 2019**

Information Management & Security Policy Summary

Information security is one of the fundamental requirements of the Trust with information processing being an integral part of its purpose because it underpins the overall IT infrastructure encompassing of the network, IT systems, telephone connections, data transfer, hardware and software. The Trust is required to ensure it has adequate expertise in Cyber security and robust disaster recovery and business continuity plans in place.

It is important, therefore, that there is a clear and robust information Security Policy in place, enabling the Trust to comply with national information legislation. This policy should be read in conjunction with the ICT Systems Use Policy.

Contents

1. Introduction

1.1 The purpose of this Information Security policy is to protect, to a consistently high standard, all information assets held by the Trust. It is a key component of Lincolnshire Partnership NHS Foundation Trust's overall information management and security framework and should be considered alongside more detailed information security documentation including, system level security procedures, security guidance and protocols and disaster recovery protocols. The policy covers security which can be applied through technology but perhaps more crucially, it encompasses the behaviour of the people who manage information in line with national requirements.

1.2 Lincolnshire Partnership NHS Foundation Trust is a mental health and social care trust providing services across Lincolnshire and North East Lincolnshire from over 70 sites. This includes a range of inpatient services and community based services. The Trust has approximately 2000 staff who either work in direct care delivery or provide a business support function (corporate services).

1.3 Information is collected and recorded in a number of mediums, including paper and electronic. The Trust has well developed infrastructures and arrangements to support information security. It shares some of these arrangements with other health care providers (NHS and Non-NHS) and has developed shared care, memorandums of understanding and information sharing protocols with these organisations. Where these are identified as part of a contractual arrangement linked to the provision of services, there is a clear expectation that partner organisations will maintain at least the same levels and approaches to Information security as the Trust.

1.4 Responsibility for information security resides, ultimately, with the Trust's Chief Executive, Executive Directors or equivalent responsible officers where these responsibilities have been formally delegated. This responsibility will be discharged through a designated member of staff who has lead responsibility for information security management within the organisation. The information security lead (SIRO) is of appropriate seniority and is an Executive Director that is a member of the Trust Board with voting rights. Equally the Caldicott Guardian is of equal seniority but also has a clinical lead within the Trust. These lead roles are formally acknowledged and will be made widely known throughout the organisation through this policy and other communications.

2. Purpose

2.1 Objectives

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the Trust is providing a secure and trusted environment for the management of information used in delivering its business.

- Clarity over the personal responsibilities around information security expected of staff working within the Trust.
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

The objectives of Lincolnshire Partnership NHS Foundation Trust Information Security Policy are to preserve:

- **Confidentiality** – Access to Data will be confined to those with appropriate authority.
- **Integrity** – Information will be complete and accurate. All systems, assets and networks will operate correctly, according to specification.
- **Availability –** Information will be available and delivered to the right person, at the time when it is needed.
- **Held securely** – data and information storage environments will be secure and managed in line with legislation and best practice guidance.

2.2 Policy Aim

The aim of this policy is to establish and maintain the management, security and confidentiality of information, information systems, applications and networks owned or held by Lincolnshire Partnership NHS Foundation Trust by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they will be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.
- Ensuring that those with a specific responsibility for information management understand what is required and are trained appropriately.
- Being aware and mindful of the increasing risk of cyber security attacks on public sector organisations and their role and responsibilities in maintaining the integrity of the Trust's information security arrangements and ensuring local business continuity plans are enabled in such an event.

2.3 Scope

This policy applies to all information, information systems, networks, applications, locations and users of Lincolnshire Partnership NHS Foundation Trust or supplied under contract to the Trust and its workers as part of their duties when employed or acting on behalf of the Trust.

3. Roles and Responsibilities

Chief Executive

3.1 Although information security and governance is everyone's responsibility, ultimate responsibility for information security resides with the Chief Executive, but on a day-to-day basis the Senior Information Risk Owner (SIRO) is responsible for managing and implementing the policy and related procedures.

Senior Information Risk Owner (SIRO)

3.2 The SIRO advises the Board on the effectiveness of information risk management across the organisation.

On a day to day basis the SIRO is responsible for managing and implementing the policy and related procedures.

Information Asset Owner (IAO)

3.3 Information Asset Owners who are responsible to the SIRO and for systems and data, will ensure that those systems and data are secure, managed effectively and in line with legislation and that an audit of security, access controls and information and data flows is carried out at least annually in their areas of responsibility. In addition that there is a business continuity plan for all critical systems (electronic and manual) that they have responsibility for.

Information Security Manager (Deputy Director of Informatics)

3.4 The Information Security Manager will:

- Have lead responsibility for information security management for the Trust, acting as a central point of contact on information security
- Manage and implement this policy and related procedures.
- Monitor potential and actual security breaches.
- Ensure that staff are aware of their responsibilities and accountability for information security.
- Ensure compliance with relevant legislation and regulations.

Caldicott Guardian (Medical Director)

3.5 The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data. The aim of the Caldicott Guardian is to ensure the organisation implements the Caldicott principles and data security standards.

Data Protection Officer (Team Leader Information Governance, Records Management and Privacy)

3.6 The Data Protection Officer is responsible for ensuring that the Trust and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer shall:

- Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, General Data Protection Regulations, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for information legislation both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of the Act across the Trust.
- Lead on matters concerning individuals right to access information held by the Trust and the transparency agenda.

Line Managers

3.7 Line Managers are responsible for ensuring that their permanent, temporary staff, volunteers and contractors are aware of:

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.
- Are up to date with an acceptable level of information governance training based on their role as well as being shown where the local business continuity plans are held should there be a need to implement them.
- Responsible for the security of their physical environments where information is processed or stored.

All Staff

3.8 All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should understand:

- What information they are using, how it should be protectively handled, stored and transferred.
- What procedures, standards and protocols exist for the sharing of information with others.
- How to report a suspected breach of information security within the organisation.
- Their responsibility for raising any information security concerns with the Information Security Manager.
- There is a need to maintain their level of knowledge and training to allow them to meet the requirements of their role in respect of information management and security by undertaking mandated annual refresh information governance and information security training.
- Each member of staff will be responsible for the operational security of the information systems they use and the information they input into it. Where changes to systems, operating processes or access rights are proposed, the IG checklist should be used to ascertain any new or additional risks (see appendix) before any changes are implemented.
- Each system user will comply with the security requirements that are currently in force, and will also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard. This includes the accuracy, timeliness and availability of data and information they are responsible for (in line with national and local standards for record keeping). They will also comply with the agreed operating guidelines/policies for each system at all times.

Contractors / Suppliers

3.9 Contracts with external contractors that allow access to the organisation's information systems will be in operation before access is allowed. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies. There is a requirement to carry out a Privacy Impact Assessments (PIAs), information security assessment and to create a Memorandum of Understanding (MOU) where necessary when PIAs have been completed. As from May 2018 PIA will be mandatory in accordance with the GDPR. Privacy impact assessment: A systematic and comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure for personal data prior to the introduction of or a change to a policy, process or procedure.

3.10 Contractors/suppliers will have completed an information governance review to a recognised national standard to offer further assurance to the organisation of the robustness of their systems and processes and must register on the Information Governance Toolkit.

4. Definitions

4.1 Lincolnshire Partnership NHS Foundation Trust will implement appropriate information classifications controls, based upon the results of formal risk assessment using the IG checklist and guidance contained within the IG Toolkit to secure their NHS information assets.

4.2 The classification Official Sensitive – Personal, will be used for patients' clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies. In order to safeguard confidentiality:

- The term "NHS Confidential" will not be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice.
- Documents marked will be held securely at all times in a locked room to which only authorised persons have access.
- They will not be left unattended at any time in any place where unauthorised persons might gain access to them.
- They will be transported securely in sealed packaging or locked containers. Users breaching these requirements may be subject to disciplinary action.

4.3 The classification Official Sensitive - Commercial, -will be used to mark all other sensitive information such as financial and contractual records. It will cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

4.4 NHS Restricted hard copy documents are to be stored in lockable cabinets, or if they are electronic they are to be stored on the H or Z drive, or SHARON.

5. Legislation

5.1 Lincolnshire Partnership NHS Foundation Trust is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of Lincolnshire Partnership NHS Foundation Trust,

who may be held personally accountable for any breaches of information security for which they may be held responsible. The Trust will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2001)
- General Data Protection Regulation (GDPR) May 2016

5.2 The Trust will maintain its annual registration with the Information Commissioner (ICO). The ICO is the UK's independent authority set up to uphold information rights in the public interest, under the Data Protection Act 1998 and provision of public information under the Freedom of Information Act 2000. The ICO investigates complaints made by the public and provides guidance for the public and organisations. If the Trust does not meet its obligations a fine or enforcement notice can be issued to the Trust. Fines received can currently be £500,000, although this will increase when the General Data Protection Regulation (GDPR) is fully implemented in May 2018.

6. Policy Framework

6.1 Mandated Information Governance and Security training

- Information security awareness training will be included in the staff induction process (to include records management and information governance).
- An ongoing awareness programme (annual mandatory Information Governance training) will be established and maintained in order to ensure that staff awareness is refreshed and updated.

6.2 Contracts of Employment

- Staff security requirements will be addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause that details each member of staff's responsibilities in respect of information security.
- Information security expectations of staff with specific responsibilities will be included within job definitions.

6.3 Security Controls of Assets

Each IT asset whether hardware, software, application or data (which includes paper) will have a named custodian (Information Asset Owner) who will be responsible for the information security of that asset, its management and its disposal (where authorised by

the SIRO). The existing custodian remains responsible for updating the asset register where the circumstances have changed in relation to the asset. This includes where the asset is no longer serviceable, has been passed to a new user, or is to be returned into stock to be reallocated. All assets remain the property of the Trust and not individual workers or managers.

6.4 Access Controls

Only authorised personnel who have a justified and approved business need will be given access to restricted areas containing information systems or stored data.

6.5 User Access Controls

Access to information will be restricted to authorised users who have a bona-fide business need to access the information.

6.6 Computer Access Controls

Access to computer facilities will be restricted to authorised users who have a business need to use the facilities. Where this access is abused or circumstances change this facility may be removed permanently or temporarily at the discretion of the SIRO.

6.7 Application Access Control

Access to data, system utilities and program source libraries will be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will depend on the availability of a licence from the supplier.

6.8 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment will be physically protected from threats and environmental hazards. Where possible this will include protecting equipment through password protection and encryption in line with national guidelines and in accordance with Trust policy on e-mail, mobile working and the computer use.

6.9 Computer and Network Procedures

Management of computers and networks will be controlled through standard documented procedures that have been authorised by the IM&T Committee.

6.10 Information Security Risk Assessment

Once identified, information security risks will be managed on a formal basis. They will be recorded within a baseline risk register and action plans will be put in place to effectively manage those risks. The risk register and all associated actions will be reviewed at regular intervals. Any implemented information security arrangements will also be a regularly reviewed feature of the Trust's risk management programme. These reviews will help identify areas of continuing best practice and possible weakness, as

well as potential risks that may have arisen since the last review was completed (see appendix for risk assessment and risk review processes).

6.11 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported through the incident management system in accordance with the Trust's risk management incident policy arrangements. All information security events will be appropriately investigated to establish their cause and impacts with a view to avoiding similar events.

6.12 Classification of Sensitive Information

See section 4

6.13 Protection from Malicious Software

The organisation will use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff will be expected to co-operate fully with this policy. Staff using mobile equipment such as laptops and iPads must ensure that they routinely visit Trust premises and connect their equipment to the network to ensure that virus protection software is updated. **Users will not install software on the organisation's property without permission from the SIRO or delegated officer. Users breaching this requirement may be subject to disciplinary action**.

6.14 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment; require the approval of the Trust's IM&T lead before they may be used on Lincolnshire Partnership NHS Foundation Trust systems. Such media must also be fully virus checked before being used on the organisation's equipment. Approved encrypted removable media must be ordered via the IT department and this must always be the first choice for users. Only Trust approved encrypted USB's/hard drives are to be used. Users breaching this requirement may be subject to disciplinary action and have their access rights removed.

6.15 Cyber Attacks

Cyber attacks (a criminal attack to attempt to damage, disrupt, steal confidential data, or request money) have detrimental effects on the Trust network and ICT systems. Despite the Trust having preventative measures in place to prevent an attack, cyber criminals are extremely knowledgeable and can occasionally out-wit technical applications; therefore it is the responsibility of staff within the Trust to remain vigilant. Any suspicious e-mails must not be forwarded to other recipients and if there is an attachment it must not be opened. I.T are to be contacted immediately. If staff come across any suspicious messages or requests on screen (e.g a message asking for a ransom) the PC or laptop is to be turned off immediately and the network cable (LAN) unplugged. I.T must be contacted immediately.

6.16 Monitoring System Access and Use

An audit trail of system access and data use by staff will be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. All access to clinical systems is monitored and audited to ensure that access is appropriate. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system
- The ability to provide service users with information regarding who has accessed their records

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

6.17 Accreditation of Information Systems

The organisation will ensure that all new information systems, applications and networks include a security plan and are approved by the SIRO and Caldicott Guardian before they commence operation and that a privacy impact assessment has been completed.

All Trust systems will also be required to adhere to Clinical Safety Standards (https://digital.nhs.uk/clinical-safety/clinical-risk-management-standards);
The following two standards, relating to clinical safety, are accepted for publication under section 250 of the Health and Social Care Act 2012 by the Standardisation Committee for Care Information (SCCI).
SCCI0129 – This standard sets clinical risk management requirements for Manufacturers of health IT systems.
SCCI0160 – This standard requires a health organisation to establish a framework within which the clinical risks associated with the deployment and implementation of a new or modified health IT system are properly managed. Appropriate assessments will be undertaken by the Trust Clinical Safety Officer as part of any system development/implementation.

6.18 System Change Control

Changes to information systems, applications or networks will be reviewed and approved by the SIRO on the advice of the Deputy Director of Informatics.

6.19 Intellectual Property Rights

The organisation will ensure that all information products are properly licensed and that they are approved by the SIRO on the advice of the Deputy Director of Informatics. Users will not install software on the organisation's property without permission from the Deputy Director of Informatics. Users breaching this requirement may be subject to disciplinary action.

6.20 Business Continuity and Disaster Recovery Plans

The organisation will ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks. Sections on procedural action in the event of the loss of computer, software or systems access will be included in all operational service business continuity and disaster recovery plans.

6.21 Reporting

The Deputy Director of Informatics will keep the IM&T Committee informed of the information security status of the organisation by means of regular reports and presentations. The ICT services lead will also provide the organisation with regular reports on reported issues through the helpdesk, network availability and downtime, system and network security assurance and planned developments.

6.22 Policy Audit

This policy will be subject to audit by the Trust's internal auditors and annual Information Governance Toolkit Assessment.

6.23 Further Information

Further information and advice on this policy can be obtained from the Deputy Director of Informatics.

6.24 Review and Revision Arrangements

The Information Security Policy will be maintained, reviewed, updated and presented to the Information Governance and Records Management Group for approval. This review will take place at least annually, or when changes are required.

6.25 Dissemination and Implementation

This policy will be disseminated utilising the Trust's current arrangements. The policy will also be disseminated through the IM&T Committee members. Implementation will be through training at induction, Information Governance Training and systems training.

There will also be awareness raising, through computer logon screens, screensavers and references made in associated policies and guidance.

6.26 Monitoring Compliance

The Trust will monitor compliance with this policy through regular audit and review and through monitoring the number and type of incidents related to information security.

7. Audit and Monitoring

7.1 Monitoring and/or audit of information systems.

Systems	**Monitoring and/or Audit**				
Criteria	Measurable	Lead Officer/Group	Frequency	Reporting to	Action Plan/ Monitoring
Application of Procedures	Internal Audit programme	Deputy Director of Informatics	Annually	Audit and Assurance	IM&T Committee
	Incident reporting	Information Governance/ Records Management Group	Bi-Monthly	IM&T Committee	Information Governance/Records Management Group
	Induction Training	Learning & Development Department	As and when required	IM&T Committee	Information Governance/Records Management Group
	Mandatory IG Training	Learning & Development Department	Annual	Board of Directors	Workforce Committee
	Audit of information and data flows	Information Asset Owners	Annual	IM&T Committee	Information Governance/Records Management Group
	System review and new system risk assessments	Information Asset Owners/ Project Leads	As and when required	Programme Delivery Group/ SDT	Operational and Strategic Delivery Teams

8. Policy Control Including Archiving Arrangements

Policy control and archiving will be carried out in accordance with the Trust's current arrangements.

9. References

- NHS Digital Information Governance Toolkit

10. Policy Approval

Name	
Job Title	
Signature	
Date	

Appendix 1

Information Governance Checklists, Privacy Impact Assessments and Information System/Asset Risk Assessments

1. Introduction

The Trust needs to ensure that it remains compliant with legislation such as the Data Protection Act 1998, NHS Standards and Information Governance Toolkit requirements with regards it's handling of Service Users, Staff and Corporate Information. The Information Governance Initial Checklist (IGC), Information Governance Key Questions Checklist, Privacy Impact Assessments (PIA) and Information Asset Risk Assessments have been developed to provide an assessment when new services are started, new information processing systems/assets are introduced or changes made to existing information systems.

2. Responsibilities

Responsibility for ensuring that Information Governance Checklists, Privacy Impact Assessments and Risk Assessments are completed, where required, resides with all Senior Managers and Department/Service Managers that are identified as Information Asset Owners (IAOs). Managers are also responsible for ensuring that relevant staff are aware of the Information Governance Checklist, Privacy Impact Assessment and Risk Assessment processes. On a day-to-day basis staff of all levels, that are introducing a new system, be it electronic or paper based, should use this document to ensure that processing remains compliant with current legislation.

3. Information Governance Checklists

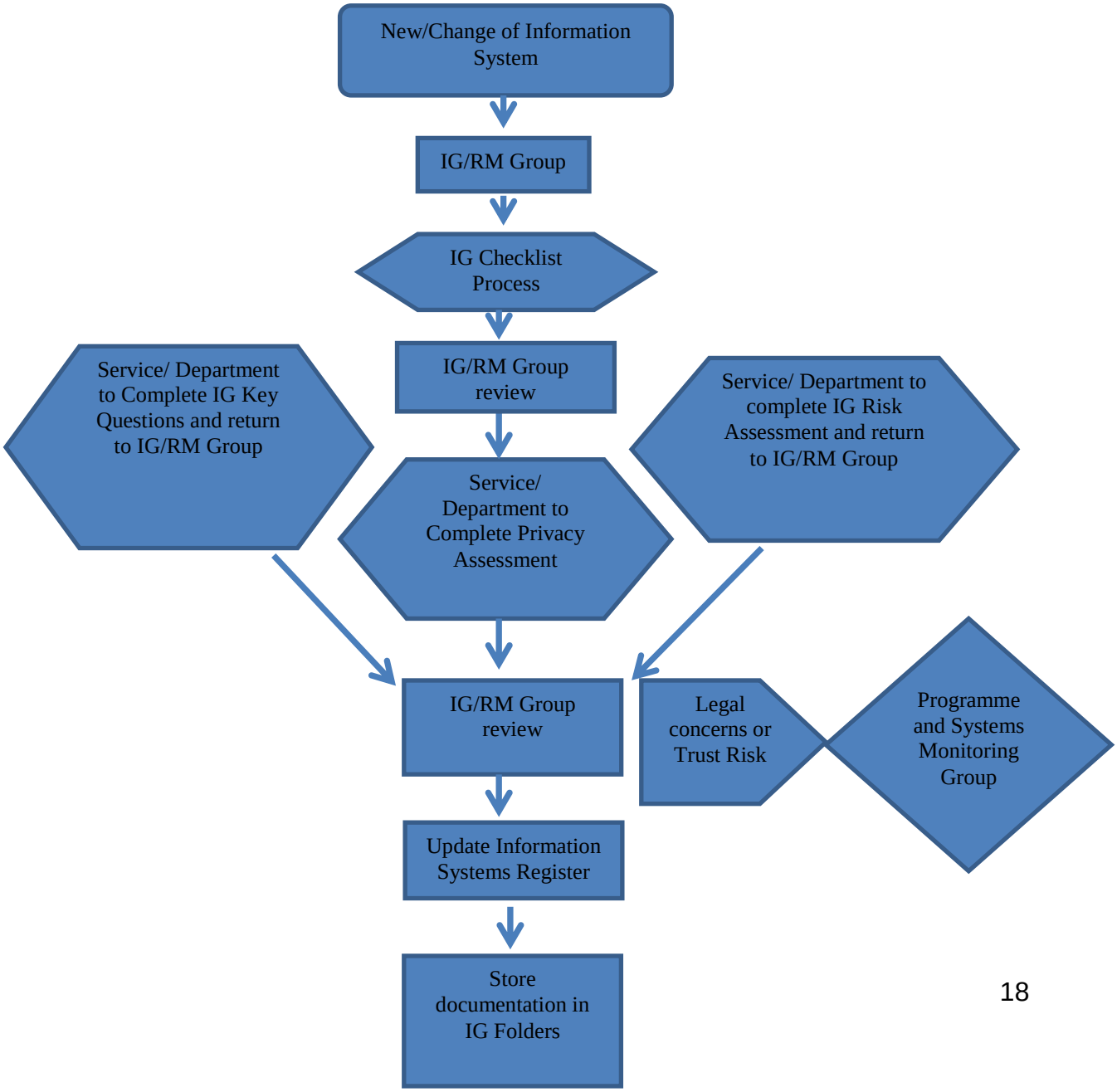
The Information Governance Checklist (IGC) provides short initial assessment which should be completed at an early stage of any new information system/asset or changes to existing information system/asset programme to make an initial assessment of privacy risk and decide if a Privacy Impact Assessment and/or an Information Governance Key Questions Checklist and Information Asset Risk should be completed. A copy of the IGC form can be found at Appendix 1 (Page 4)

4. Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. A PIA is necessary to identify and manage risks; to avoid unnecessary costs; to avoid inadequate solutions to privacy risks; to avoid loss of trust and reputation; to inform the organisation's communication strategy and to meet legal requirements. The overall PIA process is operated under the supervision of the Information Commissioners Office (ICO) who is responsible for the Data Protection Act 1998. A copy of the Privacy Impact Assessment Template can be found within the Trust's Information Management and Security Policy.

5. Information System/Asset Risk Assessment

Information, in whatever form, is a valuable asset to any organisation, it is the basis on which strategic decisions are made and daily tasks are performed. Good information handling brings great benefits, poor handling brings significant risks and compromised information can cause enormous damage to an organisation's operations and reputation. Information must be appropriately controlled and protected against the threats, non-technical as well as technical, which can affect it. Information not appropriately protected can lead to serious compliance and legal failures. A risk is the potential for harmful outcomes to impact upon business objectives, including reputation. Risk assessment is a key risk management activity that identifies, assesses and articulates risks to the organisation. Carrying out Information Asset Risk Assessments (IARA) will enable the Trust to identify, document, assess, prioritise and mitigate information handling risks which will enable risks to be managed and controls put in place to address potential information risk events or situations. A copy of the Information System/Asset Risk Assessment protocol can be found at Appendix 3.



Appendix 2

IG Initial Checklist - New/Change of Information System/Asset (IGC)

Name of Project or Service Change	
Lead Project Manager	
Other teams/staff involved	
Describe the New/Change of Information System	
Does project involve processing of Personal Confidential Data (PCD)?	
Will this processing be carried out within the UK?	
If outside of the UK – where will the data be processed?	
If yes how many records will be involved?	
What is the purpose of the processing?	
Which organisations/companies are involved?	
Which departments/services and service users are involved?	
Give an indication of the timescale for the project?	

Appendix 3

IG Key Questions Checklist – New System/Change of Information System/Asset

System/Asset Name:			
Objective:			
Is this a:	□ **New System** □ **Change of System** □ **Project**	Background: Why is this required? Is there an approved business case?	
Benefits:			
Constraints:			
Relationships: (for example, with other Trust's, organisations)			
Quality expectations:			
Cross reference to other projects:		Contact Programme and Systems Monitoring Group for info on other projects.	
Project Manager:		Name:	
		Title:	
		Department:	
		Telephone:	
		Email	
Information Asset Owner: (All systems/assets must have an Information Asset Owner (IAO). IAO's are normally Heads of Departments/Senior Managers and report to the SIRO) *Contact IG/RM Group if more information required.*		Name:	
		Title:	
		Department:	
		Telephone:	
		Email	

Information Asset Administrator: (All systems / assets must have an Information Asset Administrator (IAA) who reports the IAO as stated above.	Name:	
	Title:	
	Department:	

Contact IG/RM Group if more information required.	Telephone:	
	Email	

Question	Response	Ref to Key: IGTK, Small Scale PIA etc
1. Will the system,project or process (referred to thereafter as 'asset') contain Personal Confidential Data or Sensitive Data? If answered 'No' you do not need to complete a PIA.	□ No □ Patient □ Staff □ Other (specify):	
2. Please state purpose for the collection of the data: for example, patient treatment, health administration, research, audit, staff administration		
3. Does the asset involve new privacy–enhancing technologies? Encryption; 2 factor authentication, pseudonymisation	□ Yes □ No If yes please give details:	SS PIA (1)
4. Please tick the data items that are held in the system **Personal** **Sensitive**	□ Name □ Address □ Post Code □ Date of Birth □ GP □ Consultant □ Next of Kin □ Clinical System No □ Sex □ NHS Number □ National Insurance Number □ Treatment Dates □ Sex □ Diagnosis □ Religion □ Occupation □ Ethnic Origin □ Medical History □ Staff Data (Pay, Union) □ Other (please state):	

5. Will the asset collect new personal data items which have not been collected before?	☐ Yes ☐ No If yes, please give details:	SS PIA (5)
6. What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or sensitive data for this asset?	*Contact RM/IG Group if more information required.*	SS PIA (2 & 10)
7. Does the asset involve new or changed data collection policies that may be unclear or intrusive?	☐ Yes ☐ No	SS PIA (9)
8. Is the third party contract/supplier of the system registered with the Information Commissioner? What is their notification number?	☐ Yes ☐No Data Protection Act Notification Number: *Please check with supplier or on ICO website as below:* https://ico.org.uk/	
9. Has the third party supplier completed an Information Governance Toolkit Return?	☐Yes ☐No yes, please give percentage score: *Please check with supplier or on NHS Digital website under reports as below:* https://www.igt.hscic.gov.uk/	
10. Does the third party/supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?	☐Yes ☐No	IG TK 110
11. Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 (see appendix for definition)	☐Yes ☐No	Privacy Law Check
12. Who provides the information for the asset?	☐Patient ☐Staff ☐Others – Please specify	

13. Are you relying on individuals (service users/staff) to provide consent for the processing of personal identifiable or sensitive data?	Yes ☐No	

14. If yes, how will that consent be obtained? Please state:		
15. How will consent and non-consent be recorded?		
16. If consent is not the basis for processing which legal justification is being used?	☐Court Order ☐Public Interest ☐Other (detail below)	
17. Have the individuals been informed of and have given their consent to all the processing and disclosures?	☐Yes (explicit) ☐No ☐Yes (implicit in leaflets, on website)	IGTK
18. How will the information be kept up to date and checked for accuracy and completeness?		
19. Who will have access to the information within the system?		
20. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?	☐Yes ☐No	Privacy Check
21. If applicable, are there procedures in place for an individual's request to prevent processing for purposes of direct marketing in place?	☐Yes ☐No	Privacy Check
22. Is automated decision making used? **If yes, how do you notify the individual?**	☐Yes ☐No	Privacy Check

23. Is there a useable audit trail in place for the asset? For example, to identify who has accessed a record?	☐Yes ☐No	IGTK
24. Have you assessed that the processing of personal/sensitive data will not cause any unwarranted damage or distress to the individuals concerned? What assessment has been carried out?	☐Yes ☐No	
25. What procedures are in place for the rectifying/blocking of data by individual request or court order?		
26. Does the asset involve new or changed data access or disclosure arrangements that may be unclear?	☐Yes ☐No	SS PIA (12)
27. Does the asset involve changing the medium for disclosure for publicly available information in such a way that data become more readily accessible than before? (For example, from paper to electronic via the web?)	☐Yes ☐No	SS PIA (14)
28. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management Code of Practice for Health and Social Care 2016)		SS PIA (13)
29. How will the data be destroyed when it is no longer required?		IGTK
30. Will the information be shared with any other establishments/ organisations/Trust's?	☐Yes ☐No If yes please state who it will be shared with:	IGTK, PIA 4

31. Does the asset involve multiple organisations whether public or private sector? Include any external organisations. Also include how the data will be sent/accessed and secured.	☐Yes	☐No	
32. Does the asset involve new linkage of personal data with data in other collections, or is there significant changes in data linkages?	☐Yes	☐No	SS PIA (8)
33. Where will the information be kept/stored/accessed?	☐On paper ☐On a database saved on a network folder/drive ☐Website ☐On a dedicated system saved to the Network ☐Other – please state below:		
34. Will any information be sent off site **If 'Yes' where is this information being sent to?**	☐Yes	☐No	IGTK 208 & 308
35. Please state by which method the information will be transported.	☐Fax ☐Via NHS Mail ☐Website ☐By hand ☐Via telephone ☐external Other – please state below:	☐Email ☐Via courier ☐Via post – internal ☐Via post -	IGTK 208 & 308

36. Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)? **If yes, where?**	☐Yes ☐No	IGTK 209
37. What is the data to be transferred to the non EEA country?		IGTK 209
38. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	☐Yes ☐No ☐Not applicable	IGTK 209
39. Have you checked that the non EEA country has an adequate level of protection for data Security?	☐Yes ☐No ☐Not applicable If Yes please provide the back-up information security documentation.	IGTK 209
40. Is there a Security Management Policy and a System Access Policy in place? Please provide these policies.	☐Yes ☐No	SS PIA (11)
41. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)? **Were any risks highlighted?** **Please provide details on how these risks will be mitigated.**	☐Yes ☐No ☐Yes ☐No *If Risk Assessment completed please send with this document.*	

42. Is there a contingency plan / backup policy, or business continuity plan in place to manage the effect of an unforeseen event? Please provide a copy.	☐Yes	☐No	
43. Are there procedures in place to recover data (both electronic /paper) which may be damaged through: • **Human error** • **Computer virus** • **Network failure** • **Theft** • **Fire Flood**	☐Yes	☐No	

Appendix 4

LPFT Forensic Readiness Procedure

Introduction

The purpose of this procedure is to provide guidance on the gathering of digital evidence to support LPFT in investigations and cyber attacks.

Procedure Statement

1. Overview

1.2 This procedure reflects the high level of importance placed upon minimising the impacts of information security events and safeguarding the interests of members of the public, staff and the Trust itself.

1.3 Forensic readiness should provide suitable best evidence in support of an investigation and that the evidence is obtained in compliance with current rules, can be verified and has provable continuity. The evidence gathering needs to be professional and recorded correctly, the skills, expertise and training of the participants therefore need to be consistent with these goals.

1.4 These guidelines are applicable to all areas of the Trust and if possible / relevant adherence should be included in all contracts for outsourced or shared services.

2. Protective Marking of Evidence

Consideration should be given to the security of the evidence gathered and its protective marking classification; all data should be assessed using GSC (Government Security Classification). If it is extracted from systems that process protectively marked data, or data with special handling caveats, it should have at least the same applied. Once classified the data should be handled, stored and transferred in accordance with the scheme.

3. Roles and Responsibilities

3.1 The Deputy Director of Informatics

Is accountable for the implementation of these guidelines and process, although specific responsibility will be delegated to others within the Trust.

3.2 The Team Leader for Information Governance, Records Management and Privacy

Will be responsible for providing guidance for implementing and compliance with these guidelines and process. Encouraging all appropriate staff to follow the procedures, guidance and best practice. Identifying areas where improvements could be made in the application of these guidelines and process.

3.3 Incident Manager - (On call IT manager or as directed by the Deputy Director of Informatics)

Will take overall control of the incident and liaise with the Information Asset owners: Deputy Director of Informatics, Head of Informatics and IT Technical Lead.

3.4 Information Asset Owners (IAOs):

Will when required support the incident manager taking control of the incident and if necessary assist in the recovery of log files, emails, back up data, removable media, portable computers and network and telephone records amongst others.

3.5 IT Technical advisors

Members of the IT Department, with the relevant skills and expertise to enable the secure recovery of log files, emails, back up data, removable media, portable computers and network and telephone records amongst others. Will when required support the incident Manager taking control of the incident and assist in the investigation they will need to be aware of and adhere to relevant information governance policies and procedures.

4. Forensic Readiness

NOTE: Initially when an incident occurs, no action should be taken other than securing the scene, preventing any further data loss and ensuring that any further access is prevented. As quickly as possible a meeting should be held (either physically or virtually) including the Deputy Director of Informatics, Gold Commander (if involved), IT Technical Manager, and the Head of Informatics.

The purpose of this initial meeting will be to take stock of the incident, consider the possible outcomes and to plan an overall strategy to ensure that the appropriate individuals are responsible for the investigation and evidence gathering.

- Forensic examination of computers and digital media should be conducted by appropriately skilled technical staff, with the advice and assistance of the Deputy Director of Informatics.
- Analysis of extracted data will be considered by the Deputy Director of Informatics or Gold Command and allocated to the appropriate skill area. (Unless agreed by the IT Manager or Gold Command no analysis should occur.)
- Advice and assistance on computer related investigations will in the first instance be provided by the Deputy Director of Informatics, but if necessary external assistance should be sought, either from the system manufacturer.
- Support in disciplinary/court proceedings must be considered at all times and the gathering of evidence must comply with the current rules of evidence and legal requirements:

    - Any action taken should minimise the risk of changing data that may be relied upon in court
    - Anyone accessing original data must be competent and able to explain the relevance and implications of their action in evidence. A 2 man approach should also be used to ensure that one individual is not looking at the evidence alone.
    - A record of all activity and processes applied to digital evidence should be created and preserved so another person can follow the steps and achieve the same result.

- The person in charge of the investigations should ensure that the law and principles are adhered to.

- All activity must be appropriately documented and a time line produced, including times the activity started and finished and any actions taken that involve the copying of data or logs.
- Action should be taken to minimise the risk of either altering or deleting any evidential material; if possible all evidential material should be backed up and secured as a master copy.
- Any analysis should be conducted on a working copy of the evidential data.

5. Unable to Secure the Scene and Evidence?

5.1 Initial action if the area cannot be secured as above:

5.2 If you are able to leave everything as it is until the investigation team arrives then this is the best course; however equipment should not be left unattended or be accessed by anyone at any time. Where this is not possible the following should be applied:

5.3 <u>If the Computer equipment is switched on:</u>

- Secure the area containing the equipment
- Move people away from the computer and power supplies
- Take a photo(s) of the scene
- If the computer is attached to the network remove the network cable from the data point
- If attached, disconnect any modem
- Do not touch the mouse or keyboard
- If there are any local printers operating, allow them to finish printing (further evidence may be printing

5.4 If you have to remove equipment before the investigative team arrives, the following steps as necessary must be performed:

- Record what is on the screen and take a photograph if possible
- As a priority consider obtaining a RAM dump prior to switching off
- Switch off the computer by pulling the power cable from the computer, not from the power socket (Note: for laptops, remove the battery before pulling the power cable)
- When removing the power supply always remove the end attached to the computer and not the socket. (This will avoid data being written to the hard drive if an uninterruptable power device is fitted).
- Label and photograph (if possible) all the components in situ. If no camera is available draw a sketch plan.
- Label the ports and cables so that the computer can be reconstructed at a later date.
- Carefully remove the equipment and record serial numbers (each component will have a separate number).
- Ensure all items have signed and completed exhibit labels attached.

- Search the immediate area for diaries, notebooks or pieces of paper that may contain passwords.