**ESH/POL/53419**

Epsom and St Helier University Hospitals NHS Trust



# TRUST INFORMATION SECURITY POLICY

| | |
|---|---|
| Version: | Version 1.3 |
| Ratified by: | Information Governance Committee |
| Approved by responsible committee(s) | Information Governance Committee |
| Name/title of originator/policy author(s): | Marcus Kirby, Deputy Director ICT |
| Lead Executive(s): | Peter Davies, Director of Strategy, Corporate Affairs and ICT |
| Date issued: | 16 January 2019 |
| Review date: | January 2021 |
| Target audience: | All staff |

## Contents

# 1. INTRODUCTION

The Epsom and St Helier University Hospitals NHS Trust (Trust) is increasingly dependent upon its information systems for its normal day to day operational and administrative functions. It is therefore essential that the confidentiality, integrity and availability of Trust systems and information are maintained at a level which is appropriate to its needs. Whilst it is not possible to absolutely guarantee that all systems and information are always secure, this policy aims to reduce the risk to a minimum.

# 2. KEY AUDIENCE

All Staff

# 3. SUMMARY

The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. This policy, related policies and sub policies are aimed at providing a comprehensive and consistent approach to the security management of information across the Trust in line with legislation and NHS guidance. It will ensure continuous business capability, and minimise both the likelihood of occurrence and the impacts of any information security incidents.

This policy applies to all information assets and all records held on any medium including both paper and electronic.

The policy applies to all Trust employees and all partners, suppliers and service providers to the Trust who have legitimate rights to access and use Trust information and information systems. It is compulsory that all those who work for the Trust whether as an employee, a contractor, volunteer or a supplier comply with this policy, related policies and sub policies and the standards, guidelines and procedures that are derived from them.

# 4. THE POLICY AIMS

The Information Security Policy is intended to preserve confidentiality, integrity and availability of data.

| | |
|---|---|
| **Confidentiality** | by protecting information against unauthorised disclosure |
| **Integrity** | by protecting information against errors, omissions or unauthorised alterations |
| **Availability** | by protecting information against destruction and degradation of the service/s and making it accessible to appropriate staff when they require it |

## 5. THE POLICY

A comprehensive, systematic and reliable programme for information security management will be maintained based on the requirements of the Information Governance Toolkit. There will be annual reporting of attainment and associated improvement plans through the formal information governance structures.

Threats to information security will be identified through robust risk assessment and management arrangements and shall be a key component of its overall Information Governance strategy. Threats will be reviewed to ensure that:

- Data is protected against unauthorised access or disclosure
- The integrity and evidential value of information shall be maintained
- Information shall be available to properly authorised personnel as and when it is required

Relevant regulatory and legislative requirements will be achieved.

The Trust will have in place organisation wide service continuity plans for all information systems. This will include risk assessments to ensure that alternative fallback arrangements are identified and tested.

Relevant Information Governance training and awareness will be available to all staff.

All breaches of information security, actual or suspected, shall be recorded, reported to and investigated by an appropriately appointed, trained and experienced Information Security Officer; the Head of Information Security

The Head of Information Security will ascertain the severity of incidents and using the guidance provided by the Health and Social Care Information Centre “Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation” available via the Information Governance toolkit which can be found at https://nww.igt.hscic.gov.uk/.

Incidents that meet the criteria for reporting to the Information Commissioners Office and the Department of Health will be entered in to the reporting tool contained within the information governance toolkit.

All organisations that access the NHS network infrastructure or services provided under a national contract shall satisfy and maintain NHS Information Governance, NHS Statement of Compliance and Information Security Management conditions.

There will be adequate audit provision, based upon robust risk management arrangements to ensure the continuing effectiveness of information security management.

## 6. RELEVANT LEGAL AND STATUTORY REQUIREMENTS

6.1 Risk Assessment

The Trust will ensure that any risk identified is adequately assessed in accordance with the Trust's Risk management Policy and the associated risk management procedures so that appropriate action can be taken to reduce the risk so far as is reasonably practicable.

## 7. KEY ROLES AND RESPONSIBILITIES

7.1 Chief Executive Officer

The Chief Executive Officer has overall responsibility for the Information Security Policy within the Trust. This responsibility on a day to day basis is delegated to the Director of Strategy, Planning and Performance.

7.2 Deputy Director ICT

The Deputy Director ICT team has overall responsibility for the management of Trust ICT systems, infrastructure and for the technical aspects of Information Security liaising with Information Asset Owners as required

**RESPONSIBLE COMMITTEES**

7.3 Information Governance Committee

ICTs responsible for ensuring that the Trust has a compelling vision for ICT owned by clinicians and other senior decision makers to ensure that strategy, plans, policies and management arrangements are effective in moving the Trust towards this vision.

7.4 Business Continuity and Security Group

A sub group reporting to the Information Governance Committee is responsible for developing and testing Business Continuity plans and to manage IS security arrangements to the IG toolkit standards.

**RESPONSIBILITIES**

7.5 Application System Management

Each Information system will have a designated Information Asset Owner and Information Asset Administrator; sometimes these roles will be the same. Day to day responsibilities for enforcing the policy is devolved to the Information Asset Owner to the Information Asset Administrator(s).

7.6 IG Manager

The person responsible for ensuring that Information Asset Owners are aware of the current Data Protection legislation and with the Data Protection Principles..

7.7 System Manager

This will be the individual who routinely maintains the computer hardware and its operating system in an operational condition. The individual is responsible for maintaining the integrity of the application; their role will typically involve:

- authorising users and passwords,
- Removal of users and access rights for example when staff leave the Trust.
- setting up access restrictions within the application
- , co-ordinating the provision of training and in certain cases coordinating the operational use of the application
- ; monitoring the quality of the applications functionality
- Ensuring appropriate backups are taken and tested
- Ensuring Antivirus / Malware systems are deployed where appropriate
- Ensuring systems are appropriately patched

- In liaison with the Information Asset Owner to ensure the application is used to its fullest.

- Ensuring appropriate support agreements are in place.

- Liaising with Information services and the Head of information Security as required.

7.8 Information Asset Owners

Information Asset Owners will ensure that;

- staff are instructed in their security responsibilities
- staff using computer systems/media are trained in their use
- only authorised staff are allowed access to the departments information
- documentation is always maintained for all critical job functions to ensure continuity in the event of an individual's unavailability
- staff sign confidentiality agreements as part of their contract of employment.

- the relevant departmental systems administrators are advised immediately about staff changes affecting computer access (e.g., job function changes/leaving department or organisation) so that passwords may be withdrawn/deleted
- Provide regular written assurance to the information governance committee that computer systems they are responsible for are fit for purpose and secure.
- Liaising with Information services and the Head of information Security as required.
- Ensuring that the information Flow Mapping requirements of the Information Governance Toolkit, including risk assessment are met at least annually.
- Will ensure all information processing systems are registered with Information Services

7.9 Staff responsibilities

All staff are responsible for acting in compliance with this policy and working to ensure that all the Trust information to which they have access is managed appropriately and securely.

## 8. HOW THE POLICY WILL BE MONITORED, AUDITED AND REVIEWED

Compliance with this policy is monitored at local level and through the Information Governance Committee.

This policy will be the subject of a regular review by the Information Governance Committee which will take place at not less than yearly .

Earlier review may be triggered in response to feedback from training, regulatory changes or in response to critical incidents.

## 9. Relevant Policies and Procedures relating to IS Service Continuity

Related policies:

Information Governance Policy
Trust Information Security Policy
Freedom of Information Policy
Health Records Management Policy
Records Management Policy
Trust Asset Management Policy
IS Trust Disaster Recovery Policy
Trust Network Security Policy
IS Legal and Regulatory Compliance Policy
Trust Mobile Computing Policy
Trust Configuration Management and Change Control Policy
Trust Backup and Recovery Policy
Trust Email and Internet Use Policy
Trust Malware Policy
Trust Data Protection Policy

Trust Disaster Recovery Policy

Trust Access Control and Authentication Policy
Trust Management and Reporting of Incidents policy
Social Media Policy
Disciplinary Policy

# EQUALITY IMPACT ASSESSMENT FORM

In order to carry out an effective impact assessment it is important to examine all available data and research so that any adverse impact on disability can be properly assessed.

| | | |
|---|---|---|
| 1. Name of function, strategy, project or policy | ICT Information Security Policy | |
| 2. Name, job title, department, and the telephone number of staff completing the assessment form | Marcus Kirby, Deputy Director ICT<br>Mob: 07975 232 400<br>Tel: 020 8296 4894 | |
| 3. What is the main purpose and outcomes of the function, strategy, project or policy. | The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. | |
| 4. List the main activities of the function, project/policy (for strategies list the main policy areas) | This policy, related policies and sub policies are aimed at providing a comprehensive and consistent approach to the security management of information across the Trust in line with legislation and NHS guidance. | |
| 5. Who would benefit from the strategy/project/policy | Trust staff needing to access to IT systems and services. | |
| 6. Is it relevant to:<br>- Race Relations Act<br>- Sex Discrimination Act<br>- Disability Discrimination Act<br>- Employment Equality Regulations<br>- Religion or Belief<br>- Sexual Orientation<br>- Age | <u>Yes</u> | <u>No</u><br><br>Not relevant |
| 7. Do you think that the function/strategy/project/ policy could have a negative or positive impact on :<br>Race<br>Disability<br>Gender<br>Religion<br>Sexual Orientation<br>Age | Not applicable – there is no positive or negative impact on any of these aspects. | |
| 8. How could you minimise or | N/A | |

| | |
|---|---|
| improve any negative impact? Explain how. | |
| 9. What consultation with relevant users on this project has taken place. | N/A |
| 10. If there are gaps in your consultation and research, are there any experts/relevant groups that can be contacted to get further views or evidence on the issues. Please list them and explain how you will obtain their views. | N/A |
| 11 a) Have you involved your staff in taking forward this impact assessment?<br>11 b) How have you involved the staff | N/A |
| 12. In the light of all the information detailed in this form what practical actions would you take to reduce or remove any adverse/negative impact. | N/A |

**To be signed by the Manager completing this form.**

**Signed…… Date: 7th January 2019**
Marcus Kirby
Deputy Director ICT