

|  |  |
| --- | --- |
| Responsible Manager | Bob Bowman |
| Date of Issue | 01/02/2021 |
| Version Number | 1.0 |
| Date for Review | 01/02/2022 |
| Distribution List | All Staff |

**INFORMATION SECURITY PROCEDURE**

**Policy Statement**

Leeds Rhinos Foundation: The LRF will endeavour to maintain the confidentiality, integrity, availability, and privacy of the information it holds to ensure, the continued well-being of all

stakeholders. To achieve this the LRF will apply the principles of good Information

Security.

**Scope**

The content of this policy applies to all staff of the LRF, its third-party partners, and

associated stakeholders, who access, or authorise access to, information and

the systems utilising that information. It must be strictly adhered to.

The LRF will maintain an information security framework that:

● preserves the confidentiality, integrity, availability, and privacy of all

information held within the organisation.

● evaluates the threats associated with each information asset and system.

● selects, and implements, the correct control mechanisms to mitigate the

perceived threat to information and systems, through the LRF’s

established risk management process.

● assures that this Policy is adhered to throughout the LRF, and reviews

that the Policy is appropriate for the technological environment within that

network.

**Background**

**Information security**

Information is a vital asset to the LRF’s business, and as such requires appropriate

levels of protection. Information security seeks to protect not only information assets

but also, the infrastructure it utilises, for example information and technology

networks, systems, applications, devices, and storage media, from a wide variety of

threats. The LRF does this, through the selection of appropriate control

mechanisms, to minimise business damage, demonstrate adherence to legal and

regulatory requirements and ensure service or business continuity.

The LRF will source information security best practice from national and internationally recognised bodies

**Information security control framework**

The LRF’s control framework will draw protective capabilities from three areas.

people, process, and technology.

**People -** a key aspect of good security control is an enabled workforce made aware

of threats to information assets, and how to counter them, within the context of the

Trust’s operating environment.

**Process -** a series of actions to carry out in the event of information being accessed

by unauthorised personnel (e.g. incident management and loss of mobile equipment

reporting process).

**Technology -** the protection of information assets through automated protective

means, (e.g. secure deletion software, Identify and Access Management (IAM)

Systems or Digital Rights Management (DRM) systems).

These three aspects will be used in conjunction to form a holistic approach to security

controls, (e.g. information security awareness education will complement security

controls applied directly by people, or through automated means).

**Prioritisation of information security controls**

The appropriate controls will be put in place according to the perceived level of threat

to the individual information asset or system, or in line with its information

categorisation and/or classification. These controls will fall into three

types of security controls; fundamental, enhanced, or specialised.

**Fundamental security controls**

These are typically implemented by default and can include system hardening, patch

management, password authentication, malware protection and weekly reviews of

event logs.

**Enhanced security controls**

These are often fundamental controls that are implemented with a greater degree of

attention, functionality, management, monitoring and reporting. These can include

two-factor authentication, increased monitoring of events and more frequent reviews.

**Specialised security controls**

Additional, alternative, or unique security controls that serve a specific purpose and

provide the greatest level of protection (often required to protect particular

mission-critical information assets) (e.g. application firewalls, bluetooth encryption,

biometric authentication and continuous monitoring and alerting).

**Roles and Responsibilities**

**Senior Leadership Team**

The LRF Senior Leadership Team is responsible for approval of this Information

Security Policy, ensuring it aligns to the operational needs of the LRF and is in line

with the organisational risk appetite. They should take decisions, after gaining

guidance or advice from the Director of I&T or the Head of Information Management & Security (HIMS) in the event this policy needs to change, approval of a new policy

is necessary, or if there is an information management and security incident, for

example, a data breach.

**Director of Information & Technology**

The Director of Information & Technology is the policy owner and is ultimately

accountable for ensuring that this Policy and all information security processes and

procedures are regularly reviewed and maintained.

**Head of Information Management & Security (HIMS)**

The HIMS is directly responsible for the review, update, and maintenance of this

Policy and all information security control plans and techniques. Where necessary,

the HIMS will also facilitate the creation of new information security controls, plans or

techniques at LRF.

**Head of Compliance & Quality Assurance**

The Head of Compliance & Quality Assurance is responsible for ensuring all parts of

Information Security Policy is adhered to by the LRF and third-party partner people.

This should be done through regular audit of standards across the LRF and its

network.

**Office Teams**

The LRF promotes the use of “hot desks” across its offices to ensure we use our

space as efficiently as possible. Office Teams will undertake irregular checks of office

areas to ensure that information is not left by people in an unsafe manner, for

example, if information (electronic or physical) is left open or available to

non-authorised persons, lockers are left open, or IT devices are left unlocked.

**Departmental Line Managers**

These are responsible for the cascade of information security best practice for their

teams, work areas and attempting to influence stakeholders.

**Information Management and Security Champions**

The Champions are department or team level people with a general interest in

information management and security but are not employed in such a role. The

Champion role is additional to the person’s employed role. They are responsible for

being their team’s point of contact for all information management and security

issues. They are a communication hub between the HIMS and their team, and may

undertake or manage specific information management and security tasks as

directed (e.g. consolidate knowledge of all team information assets into the LRF

Information Asset Register and keep it up to date).

**This Policy applies to everyone working at the LRF and in our**

**network**

All people working for, or on behalf of the LRF must understand and abide by the

Information Security Policy and:

● advise managers whenever they become aware of infringements of policy

that could affect the LRF’s compliance with regulation.

5

● notify the HIMS of any serious incident that is likely to impact the operation of

the LRF as a consequence of an information security incident.

● act in a way congruent with the information management and security ethos

of the LRF

.

**Monitoring and assurance**

The LRF will review the effectiveness and managerial overhead of maintaining this

Policy on (i) an annual basis, (ii) when/if any information security incident has

occurred, or (iii) when notified of any infringement of policy that could affect the

Trust’s compliance with legislation.

**Information Management**

Information management is the overarching specialisation that includes information

security, and also privacy, within its remit. Information management and guidance

principles are dealt with in a separate policy. See NCS Information Management Policy.

**Privacy**

Privacy, and the Trust’s compliance with the European Union’s General Data

Protection Regulation (EU GDPR) and/or the UK Data Protection Act 2018, is dealt

with by a separate policy. See LRF Data Protection Policy.