Information Security Policy

Introduction

Newcastle University will safeguard its information assets through the adoption of appropriate risk mitigation strategies, in response to:

- Legal, regulatory and contractual obligations;
- Sensitivity of information assets; and the
- Current and projected threat environment.

Access to information assets controlled by the University will be open by default, unless there is a substantive reason to restrict access.

Information asset owners are responsible for establishing the need to restrict access to information assets under their control and ensuring that such restrictions are regularly reviewed (e.g. when members of staff change role).

Good information security management:

- Helps protect the University's reputation within the competitive higher education sector by building and maintaining trust in the University's operational procedures, infrastructure and supply chain; and
- Is compatible with the University's cultural values of academic and personal freedom and the responsibilities those freedoms bring.

This policy applies to all members of the University, and all other parties acting on behalf of the University.

This policy forms part of a wider framework of supporting information governance policies, including:

- The Data Protection Policy: www.ncl.ac.uk/data.protection/policy.htm
- Corporate guidelines on the use of social media: www.ncl.ac.uk/info/socialmedia/guidelines

Objectives

Newcastle University is committed to developing, maintaining and improving a systematic approach to organisational information security management in order to:

- Support its strategic objectives;
- Maintain and strengthen compliance with its legal, regulatory and contractual obligations;
- Reduce risk of incidents that may impact confidentiality, integrity and availability of information assets, by using appropriate risk mitigation strategies in response to the current and projected threat environment;
- Ensure all members of the University, and all other parties acting on behalf of the University, are aware of their information security responsibilities; and
- Ensure all suspected and actual information security breaches are reported to the Information Security/Governance Team.

Information Security Procedures provide guidance on how to comply with this policy. The Information Security/Governance Team must be contacted in situations where the required guidance does not exist.

Failure to comply with this policy, and its associated guidance, may result in disciplinary action or other appropriate sanction.

Information Security Policy

Definitions

Information assets refers to information in all forms (e.g. electronic, printed, or other), and the hardware and software tools and supporting IT infrastructure used to collect, store, process, share and dispose of that information.

Sensitivity refers to the value of information assets and the impact to the University if the security of those assets is compromised.

Threat environment refers to the different ways information assets can be compromised, and the types of compromise that can occur such as loss of:

- confidentiality (e.g. the wrong people obtain access);
- integrity (e.g. the data is accidentally or deliberately changed); and
- availability (e.g. the information is not available when needed).

Threats to information assets may be accidental or deliberate, and internal or external in origin.

Risk mitigation strategies refers to the process of deciding if risks are avoided, accepted, treated or transferred, based on a risk assessment process to determine:

- the impact and likelihood of risks occurring;
- the sensitivity of information assets;
- risk mitigation costs; and
- organisational risk appetite.

Responsibilities

University Registrar: is the Senior Information Risk Owner (SIRO) and is responsible for championing information security at Executive Board level.

Information Governance Toolkit Senior Information Risk Owner (IGT SIRO)**:** is the senior information risk owner for clinical data and is responsible for championing compliance with the NHS Information Governance Toolkit in all parts the University that handle clinical data.

Digital Campus Steering Group (DCSG): is responsible for acting as Corporate Committee on information security matters.

Audit Committee: is responsible for reviewing the adequacy of organisational information security arrangements.

Information Asset Owners (IAOs): are responsible for managing risks associated with their information assets.

Members of the University, and all other parties acting on behalf of the University: are responsible for complying with the requirements of this policy and its associated guidance.

Information Governance/Security Team: is responsible for maintaining Information Security Policy and Information Security Procedures, and providing advice on their implementation.

Policy Owner: Paul McDermott, Information Security Officer (Technical), NUIT
Approved by: Digital Campus Steering Group on 26 October 2016
Approved by: Staff Committee on 23 January 2017
Review date: 5 September 2018