Information Security Policy

Effective from 16/01/2023

---

1. Purpose

To ensure that the University's information and technology assets are appropriately secured against the adverse effects of information security failures in confidentiality, integrity, availability, and compliance.

2. What is covered by the policy?

The information security arrangements for the University's information and technology assets and the safe use of such assets.

3. Who does the policy apply to?

This policy applies to everyone with access to any University information and technology asset – including, but not limited to, regular and contingent colleagues, students, contractors, and anyone authorised to process, store, access or otherwise handle University information and technology assets on behalf of the University.

4. Roles and responsibilities

Executive Director of Finance: the University Executive Board member accountable for cyber security matters.

Registrar: is the University's Senior Information Risk Owner and the University Executive Board member accountable for data protection matters.

Chief Information Security Officer (CISO): is the University's cyber security subject matter expert responsible for advising the University on cyber security matters.

Head of Information Governance and Data Protection Officer (DPO): the University's Data Protection Officer as defined by the Data Protection Act 2018 and the University's information governance subject matter expert responsible for advising the University on information governance matters

Director of NUIT: is responsible for provisioning the necessary technology and technical controls to implement this Policy, and its associated procedures.

Information Security Committee: a sub-committee of University Executive Board accountable for the University's Information Security arrangements, oversight of the implementation of the Information Security, Data Protection, Records Management and Freedom of Information policies and the approval of changes to such policies and the Cyber Security Accountability Framework.

Information Security Operations Group: a sub-committee of Information Security Committee responsible for the implementation of the Information Security, Data Protection, Records Management and Freedom of Information policies and the approval of procedure under such policies.

Audit, Risk and Assurance Committee: is responsible for reviewing the adequacy and effectiveness of University information security arrangements and reporting its opinion to Council.

Internal Audit: is responsible for providing independent assurance to management and Audit, Risk and Assurance Committee on the adequacy and effectiveness of University information security arrangements.

Cyber Security Team and Information Governance Team: are responsible for recommending information security procedures, producing guidance, monitoring operational compliance, and providing advice on implementation of the Information Security, Data Protection, Records Management and Freedom of Information policies, and associated procedures and guidance.

Information and Technology Asset Owners: are responsible for managing risks associated with their information and technology assets in line with this Policy, its associated procedures and guidance, and the Data Protection Policy.

Dean of Translational and Clinical Research Institute: as the University's Toolkit Information Risk Officer, is responsible for the implementation of the NHS Data Security Protection Toolkit (DSPT).

Cyber Security Accountability Framework: assigns the ownership of other accountabilities and responsibilities for cyber security arrangements across the University.

5. Policy

1) Newcastle University information and technology assets shall be safeguarded through the adoption of appropriate and proportionate cyber risk mitigation procedures in response to:
   a) Legal, regulatory, and contractual obligations
   b) Sensitivity of information and technology assets, and
   c) Current and projected cyber threat environment.
2) Newcastle University shall ensure compliance with the National Cyber Security Centre Cyber Essentials.
3) In line with the procedures approved under this Policy, Information and Technology Asset Owners shall establish the need to restrict access to information and technology assets under their control, implement appropriate restrictions and keep both under regular review (e.g., when colleagues change role).
4) To the extent permitted by law, Newcastle University shall monitor usage of its IT facilities:
   a) to an extent necessary for the efficient operation and management of those facilities;
   b) to ensure compliance with its statutory obligations and;
   c) to ensure that this Information Security Policy and other University policies and procedures are adhered to.
5) The CISO and DPO shall be independent of line-management in respect of:
   a) reporting information security posture,
   b) information security risk assessments, and
   c) engaging with University officers and committees on information security related matters.
6) Information Security breaches (actual or suspected) must be reported to the Cyber Security Team and the Information Governance Team.
7) The interpretation of this Policy and related procedures rests with the CISO and DPO.

6. Related regulations, statutes, and policies

Data Protection Policy
Records Management Policy
Freedom of Information Policy
Fraud, Corruption, Bribery and Financial Misconduct Policy and Procedure
Colleague disciplinary policy and procedure
Student disciplinary policy and procedure
Procurement Procedures

7. Procedure to implement the policy

1) Information Security Committee shall be responsible for approval of changes to the Information Security, Data Protection, Records Management and Freedom of Information policies and the Cyber Security Accountability Framework.
2) Information Security Operations Group shall be responsible for approving procedures under the Information Security, Data Protection, Records Management and Freedom of Information policies.
3) In the event of a matter of urgency, the CISO or DPO shall have delegated authority to approve procedure under this the Information Security, Data Protection, Records Management and Freedom of Information policies in consultation with the NUIT Senior Management Group and at least one of: Chair of Information Security Committee, Registrar or Executive Director of Finance. Such procedure shall be reported to the next meeting of the Information Security Operations Group.

8. Monitoring and reporting on compliance

What will be monitored?	**Frequency**	**Method**	**Who by**	**Reported to**
Cyber Essentials Compliance	As agreed with Committee Chair	Report	Information Security Operations Group	University Executive Board NUIT Senior Management Group Information Security Committee Audit, Risk and Assurance Committee Business Continuity and Risk Group
Cyber Threat Environment	Each Meeting	Verbal Update	Cyber Security Team	Information Security Committee Information Security Operations Group

9. Failure to comply

1) Colleagues and students may be subject to disciplinary action.
2) Third parties may be subject to breach of contract proceedings.

Document control information			
Does this replace another policy? Yes, Information Security Policy approved by Staff Committee, 23/01/2017. New policy format; clarity for procedural approval; explicit reference to Cyber Essentials.			
Approval			
Approved by:	University Executive Board	**Date:**	10/01/2023
Effective from:	16/01/2023		
Review due –	15/01/2025		
Responsibilities			
Executive sponsor:	Executive Director of Finance and Registrar		
Policy owner:	Information Security Committee		
Person(s) responsible for compliance:	As defined within Cyber Security Accountability Framework		
Consultation			
Version	**Body consulted**	**Date**	
Cyber Security Policy V0.1-0.42	COO, Registrar, Exec Director of Finance, CIO, DPO, Cyber Security Team	19/05/2022 – 05/12/2022	
Information Security Policy V0.1	DPO	14/12/2022	
Information Security Policy V0.2	Executive Director of Finance, Registrar, Director of NUIT, DPO and Head of Internal Audit	19/12/2022	
Information Security Policy V0.3	University Executive Board	10/01/2023	
Information Security Policy V1.0	Final published version	11/01/2023	
Equality, Diversity, and Inclusion Analysis: **Does the policy have the potential to impact on people in a different way because of their protected characteristics?** No If yes or unsure, please consult the Diversity Team in People Services for guidance			
Initial assessment by:	Jason Bain	**Date:** 20/05/2022	
Key changes made as a result of Equality, Diversity, and Inclusion Analysis N/A			
Document location			
https://newcastle.sharepoint.com/hub/cyber/Shared Documents/Policy/Information Security Policy.pdf			