Data Protection Policy

Effective from 22/03/2024

1. Purpose

This Data Protection Policy outlines our commitment to compliance with data protection laws and regulations and our approach to ensuring the security and privacy of personal data.

2. What is covered by the policy?

This policy covers all data processed at the University, both verbal and written.

3. Who is does the policy apply to?

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

4. Roles and responsibilities

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

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

Head of Information Governance and Data Protection Officer (DPO): Fulfil the duties of Data Protection Officer and the University's information governance subject matter expert responsible for advising the University on information governance matters. Perform the role of the University's Caldicott Guardian.

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

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.

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.

Information Governance for Health Research Group (IGHR): to support and drive the broader information governance agenda for health research and responsibility for the monitoring the Data Security and Protection Toolkit (DSPT).

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

5. Policy

Key Definitions

Data Protection and Privacy Law: includes the Data Protection Act 2018, the EU General Data Protection Regulation (GDPR), the Privacy and Electronic Communication Regulations, the EU e-Privacy Regulation and other related legislation as may be enacted in parallel with or to replace these laws.

As the University is a global University, data protection legislation will also need to be considered in other countries as relevant, in particular the Personal Data Protection Acts of Singapore and Malaysia.

Personal Data: information that can identify a living person that is held either electronically or in paper form. This can include student records, staff employment details, research datasets and images such as those recorded on CCTV.

Data Controller: decides how and why personal data is to be used and is legally required to comply with the law.

Data Processor: processes personal data on behalf of a data controller.

Data Subject: An identifiable living individual who is the subject of personal data.

Processing: In relation to personal data, this means obtaining, recording or holding the data or carrying out any operation or set of operations on the data.

Principles and Duties

Lawfulness, Fairness, and Transparency: Personal data shall be processed lawfully, fairly, and transparently in accordance with applicable data protection laws and regulations.

Purpose Limitation: Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimisation: Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Accuracy: Personal data shall be accurate and, where necessary, kept up to date. Appropriate measures shall be taken to ensure the accuracy of personal data.

Storage Limitation: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Accountability: The University will maintain appropriate records to allow us to demonstrate our compliance with these principles.

Security: The University will have appropriate security measures in place to protect personal data, taking account of the nature of the data and the harm that might be caused if it was lost These security measures will be regularly tested, assessed, and evaluated to ensure they maintain an appropriate level of security for personal data.

Data breaches: In the event of a data breach or security incident involving personal data, the University shall promptly assess the impact of the breach, take appropriate measures to mitigate any risks, and notify affected data subjects and regulatory authorities as required by law.

Rights: Data subjects will be able to exercise fully their rights to access, rectification, erasure, restriction, portability and objection, and their rights with regard to automated decision making and profiling.

Marketing: Electronic, telephone and other marketing will be carried out in accordance with the law. Guidance is available for staff to enable them to meet these requirements.

Data Protection by Design and Default: Risk assessments will be carried out on any new systems and processes and appropriate technical and organisational measures will be implemented to ensure that data protection principles are incorporated as appropriate.

International Transfers: Transfers of personal data outside of the UK and European Economic Area will be subject to appropriate safeguards in accordance with the law.

6. Related regulations, statutes, and policies

- UK General Data Protection Regulations (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications (EU Directive) Regulations 2003 (PECR)
- EU General Data Protection Regulations (GDPR)
- Personal Data Protection Act (PDPA) (Singapore)
- Personal Data Protection Act (PDPA) (Malaysia)
- Information Security Policy
- Records Management Policy
- Freedom of Information Policy
- Risk Management Policy

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 DPO shall have delegated authority to approve procedure under the Data Protection, Records Management and Freedom of Information policies in consultation with at least one of: Chair of Information Security Committee, Registrar or Executive Director of Finance. Such a procedure shall be reported to the next meeting of the Information Security Operations Group.
4) All colleagues must undergo University data protection training biennially. Staff engaged in projects associated with the NHS Data Security Protection Toolkit must undergo annual training. Specific training requisites are documented and updated in the Training Needs Analysis document.

8. Monitoring and reporting on compliance

What will be monitored?	Frequency	Method	Who by	Reported to
Overall compliance will be monitored in line with the GDPR's Accountability requirement.	Routinely	Accountability tracking system	Information Security Operations Group	Information Security Committee Audit, Risk and Assurance Committee Business Continuity and Risk Group
Reports of any breach of this policy	As required	An investigation that might be carried out as a result of an information	Head of Information Governance/DPO	Information Security Operations Group

		security incident data breach.		Information Security Committee

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 / No If yes please state. **Yes – Data Protection Policy 2018**		
Approval		
Approved by:	Information Security Committee	**Date:** XX/03/2024
Effective from:	YY/03/2024	
Review due:	3 Years after effective date	
Responsibilities		
Executive sponsor:	Registrar	
Policy owner: (This maybe an officer or Committee)	Information Security Committee	
Policy author:	Head of Information Governance & DPO	
Person(s) responsible for compliance:	Registrar	
Consultation		

Version	**Body consulted**	**Date**
2_2 (2024)	Information Security Operations Group	14/03/2024

Equality, Diversity and Inclusion Analysis: **Does the policy have the potential to impact on people in a different way because of their protected characteristics? Yes/ No/ Unsure** If yes or unsure please consult the Diversity Team in HR for guidance	
Initial assessment by:	**Date:**
Key changes made as a result of Equality Impact Assessment	
Document location	
(eg www.ncl.ac.uk/ XXXXX etc)	