Newcastle University Data Protection Policy

1. Introduction
    a. We are required to process certain information about individuals with whom we have dealings, for our own administrative purposes and to comply with our legal obligations. For example, we need to keep personal data about our employees and students in order to carry out our function as a university.
    b. We are committed to ensuring that this processing is undertaken with respect for the rights and privacy of individuals in accordance with current data protection and privacy law.
2. Some Key Definitions
    a. Data Protection and Privacy Law
        i. This includes the Data Protection Act, the EU General Data Protection Regulation, 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.
    b. Personal Data
        i. This is 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.
    c. Data Controller
        i. The data controller decides how and why personal data is to be used, and is legally required to comply with the law. The University is the data controller for the personal data it uses.
    d. Data Subject
        i. This is an identifiable living individual who is the subject of personal data.
    e. Processing
        i. 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.
3. Principles and Duties
    a. Transparency
        i. Whenever we collect personal data, we will take appropriate measures to provide data subjects with the information required to ensure they understand the nature of the processing and how to exercise their rights in relation to that processing.
    b. Consent
        i. Where we are relying on consent as a legal basis for processing personal data, individuals' consent will be collected in a manner that ensures it is freely given, specific, informed and unambiguous.
    c. Purpose Limitation / Data Minimisation / Storage Limitation / Accuracy
        i. We will only collect and use personal data for specific legitimate purposes, and it will be kept only for as long as we need it for those purposes. We will not collect excessive or irrelevant information. We will ensure that personal data we collect and process will be accurate and kept up to date, where necessary.
    d. Security
        i. We 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.

ii. Personal data will be accessible only to those people who need to use it as part of their work. Unauthorised or unlawful access to, use or disclosure of personal data may lead to disciplinary action, and in some cases could be considered as gross misconduct. In serious cases it could also be a criminal offence.
iii. We will provide prompt and effective notification to the relevant supervisory authority and to data subjects, where necessary, in the event of a personal data breach. We will cooperate fully with any regulatory investigations that result from a breach.

e. Rights
    i. 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.

f. Marketing
    i. 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.

g. Data Protection by Design and Default
    i. We will implement appropriate technical and organisational measures to ensure that data protection principles are incorporated into the development and operation of personal data processing activities.
    ii. Data protection impact assessments will be carried out for any new processing activity that is likely to result in a high risk to the rights of the data subjects whose personal data is involved in the processing.

h. Accountability
    i. We will maintain appropriate records to allow us to demonstrate our compliance with these principles and duties, including records of processing activities under our control. A Data Protection Officer will be designated to fulfil the tasks set out in law. The Data Protection Officer will be provided with the resources and support necessary to carry out those tasks.

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

4. <u>Roles and Responsibilities</u>
    a. Registrar
        i. The Registrar has overall responsibility for ensuring that the University's legal obligations are met and has responsibility for internal and external governance and corporate accountability.
        ii. The Registrar has been designated as the officer with overall responsibility for policy compliance and is the University's Senior Information Risk Owner (SIRO).
    b. Data Protection Officer
        i. Fulfil the statutory tasks of a Data Protection Officer and report on compliance to the Registrar.
        ii. Advise on policy and draw up procedures and guidance in line with best practice.
        iii. Promote and monitor policy compliance.
        iv. Coordinate and respond to requests and queries received from data subjects.
        v. Facilitate appropriate training for all relevant staff.
    c. NUIT Leadership Team
        i. Delegated authority to approve procedures and guidance made to support this policy.
    d. Managers and Data Owners

i. Managers and data owners have a responsibility for ensuring that data protection issues within their areas are managed in a way that meets the provisions of this policy.

e. All Staff and Students
   i. Be aware of data protection requirements and what they mean to the University.
   ii. Follow the policy and procedures for handling personal data.
   iii. Consult with the Information Security Team for advice and guidance when necessary.
   iv. Report data breaches to the Information Security Team as soon as possible, in line with procedure and guidance.
   v. A breach of this policy could result in disciplinary action.

5. Relationships with Existing Policies
   a. Information Security Policy
   b. Policy on the Use of IT Facilities
   c. Records Management Policy
   d. Email Retention and Usage Policy
   e. Freedom of Information Policy

Policy Owner: John Hogan, Registrar
Approved by NUIT Leadership Team, 13th December 2017
Approved by Digital Campus Steering Group, 24th January 2018
Approved by Executive Board, 30th January 2018
Approved by Council, 19th February 2018
Review Date: 19th February 2020.