Introduction

The General Data Protection Regulations (GDPR) is EU legislation to be in force from 28 May 2018 for organisations based in EU member states, and organisations based in non-EU countries where services are provided into the EU and where EU citizens' data are processed. GDPR will therefore apply to the UK (despite our withdrawal from membership of the EU) and the UK Data Protection Bill will seek to ensure that GDPR is translated into UK legislation. In the UK GDPR replaces the Data Protection Act 1998 and seeks to update, strengthen (and in some cases simplify) existing European data protection legislation across Europe to protect the rights and freedoms of data subjects. The purpose of this Policy is to set out the key obligations placed on Northumbria University and its partners in relation to the GDPR. **Sections A-B** contain important information on how GDPR is governed and managed and monitored at Northumbria. **Sections C-D** cover data subjects' rights under GDPR and how these are protected at Northumbria, includes students, staff and third parties, and the process for making Data Subject Access Requests (SAR)

Section A: Legal, Regulation and Privacy Principles

A1.1 Northumbria University is a **data controller** under GDPR, which means that the University sets the purposes and means through which it processes the sensitive and personal data of it staff, students and other parties. This means that the University is responsible for putting appropriate technical and other organisational systems in place to ensure that the University complies with a range of responsibilities, including around:

- which data will be collected
- who it will be collected from
- whether there is a reason for no notifying data subjects or seeking their consent
- how data is processed, stored and how long it is retained for
- ensuring that third parties abide by the rules.

The data controller is responsible for ensuring compliance the six privacy principles listed at the end of this Section.

A1.2 Northumbria University is the data controller for the University's wholly-owned subsidiary companies, with such companies deemed to be processing the data on the University's behalf. Northumbria University may also be a 'joint controller' of data with another body where it operates in partnership with other UK bodies, organisations in EU member states or any other body processing the data of EU citizens, including its joint venture operations in the UK and overseas.

A1.3 As a data controller, Northumbria University is also:

- itself a **data processor** in being responsible for processing the personal data it controls.
- itself a **data processor** where it is responsible for processing personal data on behalf of another data controller, e.g., a 'lead organisation such as another HEI or partner in research, or the National Health Service (NHS).
- has formal relationships in place with organisations that are a **data processor** – responsible for processing personal data on the University's behalf.

A1.4 The Information Commissioner's Office (ICO) is the **supervisory authority** in the UK responsible for enforcement of the GDPR, and to which the University as data

controller, through its Data Protection Officer (DPO) is required to report. The ICO is an independent body which:

- issues guidance on enforcing GDPR by data controllers and processors
- requires data controllers to notify it of personal data breaches
- liaises with a data subject who lodges a complaint if the data subject feels that their rights under GDPR have not been upheld and they seek rectification or redress
- has investigative and corrective powers against data controllers, including issuing of administrative fines, with the level of fine based on the nature, gravity and length of any infringement, categories of data, and volume of data subjects affected, the extent to which the data controller was negligent, the speed and route through the ICO was informed of the breach (e.g., by the data controller or by another body or data subject), actions taken to mitigate the breach and co-operation with the ICO.

A1.5 The University upholds the six privacy principles set out in the GDPR:

1) Lawfulness, fairness and transparency • *The data subject will be told what processing will occur (transparent)* • *The data processing will match this description (fair)* • *The processing will for one of the purposes specified under GDPR (lawful).*
2) Purpose limitation • *Personal data can only be collected for specified, explicit and legitimate purposes, e.g., through Privacy Notices and clear consent procedures available to data subjects.*
3) Data Minimisation • *Personal data collected should be adequate, relevant and limited to the purposes necessary to process it*
4) Accuracy • *Personal data should be kept accurate and up to date where necessary.*
5) Storage Limitation • *Personal data should only be kept in an identifiable form and retained for as long as is necessary.*
6) Integrity and Confidentiality • *Personal data should be accurate and complete so as not to jeopardise the interests of the data subject (integrity)* • *Personal data should be collected and processed in a manner that ensures appropriate security, including protection against unlawful or unauthorised or unlawful processing, or accidental loss, destruction or damage.*

Section B: GDPR Governance, Management and Reporting

Data Protection Officer

B.1 The University as a data controller is required to appoint a Data Protection Officer (DPO) under GDPR, who also acts as DPO for the University's wholly-owned subsidiary companies. The DPO is the Records and Information Manager, who has expert knowledge of data protection law and practice. The DPO:

i. ensures that employees and students at the University are aware of their rights as data subjects, and employees and third parties' responsibilities for complying with GDPR, and will ensure staff training and awareness if delivered to meet this this requirement;

ii. is the key contact with data subjects making subject access requests (SARs);
iii. oversees and advises on GDPR compliance across the University and data processors, and monitoring of this;
iv. advises colleagues on undertaking data protection impact assessments;
v. is the spokesperson for the University as data controller on data protection matters and is the principal contact with the ICO, responsible for consulting and co-operating with the ICO on behalf of the University in the case of complaints, data privacy breaches and other matters.

B.2 The DPO is empowered to provide independent advice to the University Executive to ensure that University Executive are informed about the status of GDPR compliance, and has a direct route into that body through line-management reporting via the Head of Legal Services to the Director of Strategic Planning. The DPO also reports to the Senior Information Owner Risk Owner (SIRO) in relation to mitigation and notification of personal data breaches.

Project Board and Information Governance Group

B.3 A Project Board reporting into the University's Transformation Programme Board of the University Executive is in place to oversee the implementation of the GDPR at the University. The Project Board comprises senior representatives from across the University with responsibility for GDPR project management, compliance and/or includes key information asset owners or their representatives. The Project Board will continue for a period following the GDPR coming into force in May 2018, to monitor how effectively it is being embedded. Steady state arrangements will then be overseen by the Information Governance Group.

B.4 Information Governance Group is a body of the University Executive. Chaired by the Senior Information Risk Owner (SIRO), the Group has responsibility for information governance policy development and monitoring, and will:
i. provide advice on the development of new/revision of GDPR policy, including those elements which have wider information governance implications for the University;
ii. monitor the effectiveness of GDPR implementation, and new and emerging legal and policy requirements and operational implications once the Project Board has been disbanded in later 2018;
iii. report major GDPR statutory, policy, resourcing and staffing, incidents and breaches to the University Executive for decision, to enable action where necessary, including commissioning post-incident reviews.

University Executive and the Board of Governors

B.5 The University Executive is responsible for:
i. promoting a University-wide culture of data privacy and effectiveness as identified in the six data privacy principles in A1.5 above, in exercising accountability and compliance;
ii. statutory and regulatory GDPR compliance on behalf of the University, and ensuring that any risks are effectively managed, and data breaches managed and reported to the Information Commissioner's Office as appropriate. Alongside the governance framework identified in B.3-B.4, role-holders on the University Executive through the role of the Director of Strategic Planning and Senior Information Risk Owner (SIRO) (Head of Governance) are responsible for

overseeing GDPR compliance, and are advised by, and support the Data Protection Officer (DPO). See B.1-B.2. Executive Management responsibilities are met in conjunction with other University Executive members, the wider Senior Management Group including the Director of IT and all information asset owners.

B.6 The Board of Governors of the University is ultimately accountable for legal compliance for GDPR and the financial and wider implications of non-compliance and data breaches. In undertaking its role, the Board will:

i. seek assurance from the University Executive on any aspect of GDPR policy and compliance, by any format it requires, including reporting into the Board or a relevant committee, namely Audit Committee which may request reports, audits and investigations to assess the adequacy of GDPR risk controls;
ii. in exceptional circumstances, enable the DPO to have direct access to the Chair of the Audit Committee in the first instance (and internal auditors), where the DPO judges that the University Executive has failed to adequately address risks presented to it related to GDPR, including data breach incidents.

Privacy by design and default, Data Protection Impact Assessments/Privacy Impact Assessments

B.7 The University as a data controller will adopt and implement measures to ensure 'privacy by design' as the means of ensuring that privacy and data protection principles, considerations and controls are systematically and automatically built into the projects from the start and that subsequent, development and maintenance of systems and projects undertaken by the University design these in.

B.8 Privacy by default means that the standard default in the development, review and maintenance of all systems housing personal data is to ensure a high bar is automatically set for privacy settings and controls built into the University's systems.

B.9 The University is required to undertake Data Protection Impact Assessments (DPIAs), which supersedes previous guidance issued by the ICO for data controllers undertaking Privacy Impact Assessments (PIAs). DPIAs are a structured means of ensuring privacy by design and default is built as a requirement into 'high risk' and/or 'large-scale' data processing activities undertaken by the University. A separate policy exists on Privacy by Design and Default, and DPIA procedures.

Incident Response Management and Reporting

B.10 The University will identify, respond to and report personal data breaches in a rapid and robust way, to minimise the impact on data subjects and the wider security and integrity of personal data held by the University.

B.11 A personal data breach under the GDPR is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

B.12 The identification of breach may be identified by a range of parties including staff, students a member of the public, as an result of an audit or investigation exercise or by the affected data subject (s) and should be reported immediately to the DPO. The DPO will notify relevant role-holders, including the SIRO, the relevant asset owners and University Executive of an incident deemed to be serious or material based on a series of criteria and indicators. An incident response plan will be produced under the

supervision of the DPO to [a] understand the incident and its impact [b] take action to rectify the breach including informing affected data subjects and other parties and [c] minimise any further impact and undertake post-incident review to introduce measures to limit the likelihood of re-occurrence.

B.13 The DPO is required to report the incident to the ICO of any personal data breach without undue delay and, where feasible, within 72 hours of being made aware of it, if the personal data breach is likely to result in a risk to the rights and freedoms of data subjects. Reporting of breaches to the ICO which do not meet this threshold may also be reported on the judgment of the DPO, where appropriate in conjunction with the SIRO, the University Executive and other parties.

B.14 A separate Data Breach Management and Reporting Policy is published.

Section C: The rights of data subjects and the six conditions of processing data

C.1 The University's policies and systems are designed to ensure the rights of data subjects under the GDP are upheld. These are the 'rights' to: **information, access, rectification, erasure, restriction of processing, notification, data portability, object and appropriate decision-making**. These rights are summarised below:

The right to information • The University will provide a minimum level of information to data subjects to demonstrate that their personal data is fairly collected and processed.
The right to access • The University will provide data subjects with access to information about them: a copy of their personal data, the purposes of processing their data; categories of data being processed and any third parties that might receive their data.
The right to rectification • The University will rectify and inaccuracies in personal data held about data subjects: incomplete or incorrect data.
The right to be forgotten (erasure) • The University will erase and thereby stop processing personal data where it is no longer necessary for the original reason for its collection and processing; when a data subject withdraws consent to do so; when the individual objects to the processing and there is a no legitimate interest to carry on doing so; where it is being unlawfully processed; to comply with a legal obligation, where it is being processed to offer information services to a child. • There are legitimate reasons that the University may refuse to comply with a request for erasure, where freedom of expression and information overrides this, to comply with the law and act in the public interest: including for public health, archiving and scientific, historical research or statistical purposes, making or defending legal claims.
The right to restrict processing • The University will comply with the data subject's request to restrict the processing of their personal data if the data subject: challenges the accuracy to enable the accuracy to be proven or corrected; proves that the processing is unlawful but they do not wish to it be erased.
The right to notification • The University is responsible for ensuring that its data subjects are notified of specific activities linked to the processing of their data, and that third parties are

notified if the data subject exercises any of their rights. Compulsory areas of notification of the data subject by the University include where the University alters, restricts the processing of, or removes personal data, unless this is impossible or involves disproportionate effort. • The University will also notify third parties to which they have disclosed information where the data subject exercises their rights to alter, restrict or remove their data.
The right to data portability • Data subjects of the University can request copies of the personal data held on them by the University in a useful electronic format as a means of improving the accessibility of information. The data subject has the right to transmit his/her data to another controller without objection or barriers from the University. The information should already be held by the University in a structured, automated system as this right only applies where processing of the data is based on the data subject's consent or fulfilment of a contract to which they are party.
The right to object • Data subjects have a right to object to processing of their data by the University. The University is responsible under such circumstances for demonstrating legitimate reasons for processing the individual's data which override the interests, rights and freedoms of the data subject, or for legal claims purposes. • Data subjects have the right to object to specific types of data processing: including direct marketing, where the University relies on any of legitimate interests, the wider public interest and for research and statistical purposes. • This right will be published separate publication which is standalone from this Policy, and for online services, there will be an automated way for individuals to raise their objection.
The right to appropriate decision making • Data subjects have the right not to be subject to decision-making about them based solely on automated processing of data held, including profiling which produces legal or other significant outcomes that affect them. Intervention between the data subject and an individual working on behalf of the University is a request that data subjects can ask to be fulfilled, to enable them to obtain an explanation to and challenge a decision.

The six conditions of processing personal data

C.2 GDPR introduces six 'conditions' or bases on which the University may lawfully process the personal data or staff, students and other parties. The University will be explicit about which of the conditions are being used by the University in processing such data, as a basic right to information of data subjects as identified above. Privacy notices relevant to specific processing activities of a data subject's personal information will be one key means of communication.

Lawful processing conditions	
1	Consent of the data subject
2	Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
3	Processing is necessary for compliance with a legal obligation
4	Processing is necessary to protect the vital interests of a data subject or another person
5	Processing is necessary for the performance of a task carried out in the public

	interest or in the exercise of official authority vested in the controller
6	Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are not overridden by the interests, rights or freedoms of the data subject.

C.3 As a public authority and an exempt charity, the University undertakes a wider range of statutory functions related to delivering education, research and education of individuals, including entering into contracts and agreements with registered students, contracts of employments (contracts of services) and a range of contracts for service or supply of goods with a range of external parties. On this basis, it would be expected that the University would use several of the processing conditions identified in the table overleaf, including, but not limited to: consent, processing to perform a contract, processing to comply with the law and processing for the purposes of the legitimate interests of the University as a public authority and charitable body. The University will be clear through privacy notices and other communications which of the conditions of processing it has decided to use to process specific personal data and the reason for this. Data subjects have the right to object to a condition of processing, at which point the University would review the basis for that request.

Consent

C.4 Gaining consent from the data subject by the University to process their data is discussed separately as it is cited as one the most important conditions for processing a data subject's personal data under GDPR. The University has procedures in place for gaining the consent of data subjects to process their data, where the University is expecting to use consent as the basis for processing a data subject's personal data. The University complies with the GDPR definition of consent which means any freely given, specific and therefore identify the exact informed and unambiguous indication where the data subject signals clear agreement to the processing of personal data relating to him or her, for the purposes intended. Consent therefore requires specific and positive opt-in by the data subject and is not given by pre-ticked boxes or any other form of consent by default or non-response by the data subject.

C.5 The University has procedures in place for recording evidence of where consent is given by the data subject, in whatever specific and explicit format in which the consent of the data subject is captured.

C.6 The University has procedures in place to enable data subjects to readily and accessibly exercise their right to withdraw consent they have previously given, at any time. As an outcome of exercising this right, the University will:

i. stop processing the personal data for which consent had previously been given;
ii. identify whether there are other grounds on which processing of the data can be given.

Whatever the outcome, the University will inform the data subject of its intended actions, including that the data subject has a right to object to any of the other conditions of processing that the University intends to use to process the data.

Section D: Data Subject Access Requests

D.1 The right of access to information from a data controller by a data subject is covered in C.1 above. The University therefore has appropriate processes in place to ensure

data subject access requests (SAR) are dealt with in line GDPR. Following a subject access request, an individual has the right to obtain confirmation that their data is being processed by the University, as well as access to that data and any supplementary information.

D.2 A SAR can be made in any format or communication method, including telephone, e-mail and other electronic communications. The following key points apply in making a SAR:

i. Any member of staff can receive a SAR and al requests must be passed to the DPO.
ii. it is reasonable for the DPO to request and be provided with proof of identity from the data subject making the request, and any other such enquiries to enable the DPO to judge whether the person making the request is the individual to whom the personal data relates (or a person authorised to make a SAR on a data subject's behalf)
iii. there is no fee for a SAR unless the request can be reasonable deemed to be unfounded or excessive in which case the University may charge a reasonable administrative fee. A fee may be charged if further copies of material provieded to the SAR are requested by the data subject;
iv. the University will respond to SARs without delay and at the latest within one month of receipt of the request. In exceptional circumstances, where a SAR is particularly complex or multiple, the University may notify the data subject that it is extending the period to respond by up to two further months, with the reasons for this and timescales within the extension limits;
v. the data provided back to the individual making the SAR will be provided electronically, unless requested to be provided in another format by the requestor at the time of the request.
vi. multiple of bulk SARs received willy be considered individually and responded to appropriately.
vii. the University can withhold personal data if disclosing it is exempt from disclosure under the UK Data Protection Bill or where disclosure would adversely affect the rights and freedoms of others.

D.3 A template and detailed procedures for submitting SARs is available online on the Data Protection web pages.

Approved by:	University Executive September 2017
Re-approval:	Every three years (or sooner if required by legislative, regulatory or material organisational change)
Policy Owner:	Adam Dawkins + Duncan James