

Newman University Data Protection Policy

The Data Protection Policy is to be read in conjunction with the [Data Protection Glossary](#) and [the Information Classification Table](#). A list of related documents is section 12 of this policy. All Article numbers in this policy relate to the UK GDPR.

1. Background

- 1.1** The UK General Data Protection Regulation (UK GDPR) underpins the Data Protection Act 2018 (DPA 2018). The UK GDPR and the DPA 2018 replaced the UK's Data Protection Act 1998. The UK GDPR is designed to harmonize with data privacy laws across Europe, to protect and empower all citizens' data privacy and to reshape the way organisations approach data privacy.
- 1.2** As defined in the DPA 2018 and Article 2 of the UK GDPR the material scope encompasses the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.
- 1.3** As defined in the DPA 2018 and by Article 3 of the UK GDPR, the territorial scope encompasses all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It also applies to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the EU.
- 1.4** As explained by the [Information Commissioner's Office website](#), 'personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information. Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR. Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.'
(ICO website June 2019)

2. Introduction

- 2.1** Newman University needs to process personal data in order to deliver its core learning, teaching and research functions, operate effectively as a business and meet legislative, contractual and statutory obligations.

The personal data relates to:

- past, present and prospective students including alumni and students of collaborative partners whose programmes are validated by Newman University
- past, present and prospective employees

- regulatory bodies
- suppliers
- research subjects
- supporters and others with whom it has dealings.

2.2 Under the General Data Protection Regulation (UK GDPR) and DPA 2018, the University is a data controller and must comply with data protection legislation.

3. Purpose

This policy helps provide the demonstrable commitment to, and support of, compliance with data protection legislation by the Board of Directors and University Council. Compliance with data protection legislation fits with the University's motto of 'ex umbris in veritatem' (out of the shadow into truth) and its mission to respect and encourage the individual integrity of everyone who is a part of the life of the University. As a Catholic University we seek to make a positive difference to the individuals and communities through the contribution of our staff, students and graduates, and this includes upholding the data protection principles and facilitating the rights of data subjects. Additionally compliance with data protection legislation shapes efficient working practices and significantly reduces the risks of an information security breach, which in turn reduces the risk of a causing harm / distress to data subjects, reputational damage, financial damage and undertakings from the Information Commissioner's Office.

4. Scope

This policy applies to all those individuals and organisations that process personal data on behalf of the University, including but not limited to:

- employees, consultants, contractors and temporary workers
- students performing paid or voluntary work for the University
- organisations associated with, and officially recognised by, the University
- third parties associated with the University, such as research collaborators.

5. Data Protection Principles and Rights

5.1 Accountable, lawful processing of personal data is vital to the successful operation and reputation of the University, and for maintaining the trust of our students, employees and other stakeholders. The University is committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, the University will ensure that personal data is handled appropriately and consistently.

5.2 In accordance with the data protection **principles** of the UK GDPR and DPA 2018, Newman University will ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data shall be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR and DPA 2018 in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

5.3 Newman University, as a data controller, shall be responsible for, and be able to demonstrate, compliance with the principles of data protection legislation.

5.4 All processing of personal data by third parties on behalf of the University, where the University is data controller, will be covered by appropriate contract or data sharing agreement and will include adequate data protection clauses.

5.5 Where the lawful basis for processing personal data is consent, a record of the consent will be kept for as long as the personal data is kept.

5.6

5.6.1 Data subjects have **rights** regarding data processing, and the data that is recorded about them. The University facilitates the rights as they are defined by the [Information Commissioner's Office](#):

- The right to be informed (Article 14)
- The right of access (Article 15)
- The right to rectification (Article 16)
- The right to erasure (Article 17)
- The right to restrict processing (Article 18)
- The right to data portability (Article 20)
- The right to object (Article 21)

Rights in relation to automated decision making and profiling (Article 23).

NB. The University does not carry out any automated decision making or profiling, however the reference to the Article 23 rights remains in the policy in order to ensure that the University facilitates those rights should it become applicable.

5.6.2 The main way that the Article 14 'right to be informed' is fulfilled is through the timely provision of privacy notices. The University website hosts privacy notices relating to all collection of personal data including, but not limited to:

- [Privacy Notice for Enquirers](#)
- [Privacy Notice for Applicants](#)
- [Privacy Notice for Students](#)
- [Privacy Notice for Alumni](#)
- [Privacy Notice for Professional Contacts](#)
- [Privacy Notice for Employees](#)

5.6.3 The Article 15 'right of access' is detailed further on the external webpage <https://newman.ac.uk/knowledge-base/what-is-a-data-subject-access-request-dsar-and-how-do-i-make-one/> Data Subject Access Requests (DSARs) are processed by the Data Protection Officer, who liaises with staff as appropriate.

5.7 The University has procedures to facilitate the data protection principles and rights of the data subject appropriately. Staff must follow the procedures provided on the Newman website and intranet and ask their Data Champion (i.e. Data Protection Task Group representative), manager or Data Protection Officer (in that order) if they are unsure of any procedure. The Data Breach Reporting Procedure and Data Breach Incident Management Procedure are referenced in section 10 of this policy.

5.8 If a data subject contacts any part of the University to exercise any of their rights, the person contacted should liaise with the Data Protection Officer for advice or the data subject should be put in direct contact with the Data Protection Officer (dpo@newman.ac.uk, 0121 387 4567 or Teams 4567), who will enable them to exercise their rights.

6. Sharing of Personal Data

6.1

Ensuring that personal data is shared appropriately is vital to the successful operation and the reputation of the University, and for maintaining the trust of our employees, students and other stakeholders. In order to achieve this, the University will:

- Undertake a data protection impact assessment screening for any new initiatives that involve the sharing of personal data. Where sharing is likely to result in a high risk to the rights and freedoms of natural persons (particularly where new technology is involved) a full data protection impact assessment will be completed.
- Ensure that the sharing of personal data is necessary to achieve the identified objective(s). Anonymised or pseudonymised data will be shared where the identification of data subjects is not required.
- Implement information classification with procedures for the secure sharing of 'restricted information' and 'highly restricted information'.

- Share the minimum amount of personal data required to achieve the objective(s) in a practical way.
- Provide data subjects with privacy notices and, where data subjects have a choice; seek consent for the sharing of their personal data.
- Record all decisions to share personal data with organisations other than Newman University.
- Ensure that a written agreement (i.e. contract or data sharing agreement) is in place with external parties where personal data is shared on a systematic basis or there is a large scale transfer of personal data. Such agreements will, as a minimum, include:
 - The classes, or specific items, of personal data to be shared
 - The source(s) of the personal data
 - The objective(s) of the data sharing arrangement
 - The lawful basis for sharing the personal data
 - The individuals/groups that will have access to the personal data
 - The methods by which the personal data will be transferred, including any controls for protecting the data from loss, destruction or unauthorised access
 - The frequency with which the personal data will be shared
 - Storage requirements for the personal data, including any controls for protecting the data from loss, destruction or unauthorised access
 - The parties' responsibilities for ensuring the accuracy of the personal data
 - Retention and disposal requirements
 - Arrangements for enabling data subjects to exercise their rights
 - Processes and procedures for handling information security incidents.

6.2 Sharing of personal information with a student's nominated person

- Newman University has a requirement to treat all students as adults and does not act in loco parentis ("in the place of a parent") in relation to students, regardless of their age. In accordance with data protection laws there are limited situations where the University shares personal information about students or discusses their circumstances. Outside of an emergency situation*, the University will only share such information with a student's nominated person (for example a partner, relative, friend or associate) with explicit written consent from the student, where the University is satisfied that this consent has been provided voluntarily by the student and that they have not been coerced into providing this consent. The student needs to provide written consent via their Newman University email account or in person, as decided by the relevant University service or area. This consent allows the University to share personal data about the student with the student's nominated person but does not permit that person to act on behalf of the student. The Complaints Policy should be consulted for information about acting on behalf of a student in regard to a complaint.
- In accordance with the Policy for students under the age of 18 (on the University intranet and available by request to the Deputy Registrar) the University requires the contact details of a parent/guardian for all students under the age of 18. Although those under 18 are regarded as children under UK law, they still have

the legal right for information about them not to be disclosed without their explicit written consent as above. The University therefore requires all students under the age of 18 years to provide consent for the disclosure of appropriate information to their parent or guardian, upon commencing their studies. This consent will remain in force until the student's 18th birthday.

- If someone submits a Data Subject Access Request on behalf of someone else, the University needs to satisfy itself that the person making the request has the data subject's permission to act on their behalf and that the data subject wants the DSAR to happen. More information about DSARs is found on the [Data Subject Access Request page](#) of the Newman University website.
- N.B. References to written consent may be interpreted in an appropriate way, agreed by all parties, to take account of disabilities.
- An emergency situation refers to a situation where vital interests would be an applicable lawful basis for sharing personal data.

7. Appointment and Support of the Data Protection Officer (DPO)

The University has appointed a Data Protection Officer (DPO) who is able to fulfil the tasks referred to in Article 39 of the UK GDPR. The University will enable the effective performance of the DPO's tasks and ensure that the DPO is given sufficient autonomy, time, resources and support to carry out their tasks effectively, including active support by senior management. The University will also ensure that the DPO is 'involved properly, and in a timely manner, in all issues which relate to the protection of personal data', that the opinion of the DPO is given due weight and that the DPO is consulted promptly once a data breach or another incident has occurred.

8. Roles and Responsibilities

8.1 The Board of Directors and University Council will ensure that the purposes and means of processing of personal data for which the University is data controller are determined in compliance with legislation.

Responsibility for ensuring implementation of, and compliance with, this policy will be in accordance with the University's line management structure.

8.2 All individuals and organisations that process personal data on behalf of the University will comply with this policy and associated data protection, information security, information management and information technology regulations, policies, processes and procedures.

8.3 The Data Protection Officer (DPO) is an advisory role working to ensure that Newman University complies with the requirements of the current data protection laws. The Data Protection Officer reports directly to the University Secretary and Registrar.

The DPO will:

- inform and advise all members of staff on their obligation to adhere to the data protection laws when dealing with personal data
- monitor compliance with the data protection laws
- advise and inform on data protection impact assessments (DPIA), including monitoring performance of DPIAs against the requirements of the data protection laws.
- liaise and cooperate with the supervisory authority (the ICO). This requires an appropriate level of independence and must not be influenced by other roles of any level.
- be the point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.
- contribute to the development and maintenance of all Newman University data protection policies, procedures and processes in relation to the protection of personal data.
- advise management on the allocation of responsibilities internally to support ongoing compliance with the data protection laws
- ensure training and awareness is available and delivered to all members of staff involved in processing operations relating to personal data.
- regularly monitor compliance with the data protection laws by conducting audits of processes relating to personal data, and report to the University Secretary and Registrar, and University Council (via the Audit Committee)
- be the lead point of contact for data subjects with regard to the processing of their personal data including the facilitation of their rights.
- monitor compliance with the Newman University Data Protection Policy and develop/advise on procedures for effective security.
- advise senior management on the allocation of information security responsibilities.
- develop/advise on formal procedures for personal data reporting incidents and investigations
- contribute to the business continuity and disaster recovery planning process
- advise on and monitor the safeguarding of organisational record management, (Retention and Disposal Schedules)
- work with all business areas (through Data Champions) to ascertain the extent to which personal data is collected, held and/or used in Newman University, and that it is properly controlled and safeguarded from loss of confidentiality, integrity or availability from any cause.
- ensure that records of the processing are kept by Newman University as detailed in Article 30 mentioned above.
- advise the controller of its obligation to issue privacy notices to data subjects at the point of collection of their personal data under Articles 13 to 15.
- plan and schedule data processing audits regularly, monitoring core activities to ensure they comply with the data protection laws
- be the main contact point for employees and, with the assistance of the Data Champions, liaise with all members of staff on matters of data protection.

- bring to the attention of the University Secretary and Registrar any matters which are potential risk factors to the proper safeguarding of personal data within Newman University.

The Data Protection Officer is authorised to have access to all Newman University's systems relating to the collection, processing and storage of personal data for the purpose of assessing the use and security of personal data. The Data Protection Officer may expect the cooperation of all staff in carrying out these duties, including access to systems and records. In the event that cooperation is not being forthcoming, the Data Protection Officer will report to the University Secretary and Registrar accordingly or, where necessary, the Vice-Chancellor / Chair of University Council.

8.4 The University Secretary and Registrar is an accountable role and is concerned with the management of all information assets held by the University. With regards personal data, the University Secretary and Registrar has overall responsibility for:

- the processing of personal data (of which the University is data controller) in compliance with data protection legislation, including the appropriate determination of the purposes of processing personal data, and the means by which any personal data processing activity is done
- ensuring that the DPO is involved properly, and in a timely manner, in all issues which relate to the protection of personal data, that the opinion of the DPO is given due weight and that the DPO is consulted promptly once a data breach or another incident has occurred.
- the management of data protection risks
- planning, implementing and progressing the University's data protection initiatives
- managing the implementation of essential elements of data protection legislation, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing and notification and communication of data breaches
- managing the response to breaches of data protection legislation
- ensuring that an effective monitoring and reporting framework is established with regards data protection compliance, and that information asset owners are designated, perform their roles and report regularly on data protection compliance in relation to their respective information assets and business units
- ensuring that no individual is given access to personal data without having undertaken appropriate training and read relevant policy and guidance.
- be pro-active in seeking further information / knowledge to further their professional development regarding data protection.

The University Secretary and Registrar will also play a key role in fostering a data protection culture within the University.

8.5 Information Owners (i.e. managers) are to:

- ensure that personal data held within their respective areas are processed in compliance with this policy
- identify and manage data protection risks within their respective areas
- ensure that no individual is given access to that personal data without having undertaken appropriate training and read relevant policy and guidance
- ensure that local processes and procedures are developed, implemented, followed and regularly reviewed
- be pro-active in seeking further information / knowledge to further their professional development regarding data protection.
- request advice from the DPO wherever necessary
- monitor and report on compliance in their areas as required by the University.

8.6 All employees / staff of the University are:

- responsible for their own compliance in processing personal data and other information. Non-compliance can result in disciplinary procedures.
- expected to be pro-active in seeking further information / knowledge to further their professional competence. All areas have at least one representative on the Data Protection Task Group. Advice can be sought from these representatives as well as the DPO.

8.7 Third parties processing personal data on behalf of the University will comply with this policy alongside any specific terms and conditions agreed contractually.

9. Training

9.1 Newman University is committed to providing adequate data protection training to its employees in order to help protect the rights and freedoms of individuals in accordance with the provisions of the UK GDPR and DPA 2018.

9.2 All employees of the University whose work involves accessing personal data will:

- be informed of the expectation that they will follow the Data Protection Policy and its associated policies and procedures. This expectation will also form part of the contract of employment.
- be required to undertake the University's online Data Protection module. If an employee declines to undertake the module or does not pass the test after multiple attempts, HR will investigate and where the reason for this is deemed unacceptable by the University Secretary and Registrar, this may result in disciplinary proceedings.
- Be provided with appropriate training and / or clear procedures for compliant processing of personal data according to their role.

Visiting Lecturers and External Examiners are required to undertake the University's online Data Protection module within two months of the start of their contract unless they can evidence they have completed similar training in the past two years.

For casual staff such as agency temps, whose role may involve accessing personal data, the onus is on managers to ensure that such staff are aware of their responsibilities.

Training is organised through the Learning and Development Manager, however it is the responsibility of a line manager to ensure their staff undertake the relevant training.

- 9.3** All employees whose work does not ordinarily involve accessing personal data will be given bespoke training and / or required to follow data protection procedures relevant to their role. This includes employees and casual workers such as bar and catering staff, cleaners, housekeepers, maintenance staff, porters, security officers, student ambassadors and other student volunteers.

10. Data Breaches

Any data breaches or suspected data breaches should be immediately managed and reporting in accordance with the [Data Breach Incident Response and Reporting Procedure](#) available on the intranet and internet. Third parties will report any data breaches or suspected data breaches to the University via telephoning the DPO on 0121 387 4567, if there is no answer, emailing dpo@newman.ac.uk. A third party reporting a data breach or suspected data breach must also inform their University point of contact by phone or email. Breaches will be managed in accordance with the Data Breach Incident Management Procedure, which includes, where necessary, notifying the ICO within 72 hours of a breach being known.

11. Breaches of Policy

Failure to follow any of the applicable University policies by staff / employees may result in disciplinary action. A data breach by a third party may result in a termination of contract and/or compensation claim.

11. Policy Review and Maintenance

This policy will be reviewed by the University Secretary and Registrar and DPO annually or sooner should there be a significant change in legislation, strategy or organisation. Major changes will be approved by University Operations Team or University Council.

- 12.** This policy is related to the following policies and procedures:

[Audio Recording Advice for Minute Taking](#)

[Bring Your Own Device \(BYOD\) Policy](#)

[Computing and Networking Facilities: General Conditions of Use](#)

[Confidential Waste Procedure](#)

[Data Breach Reporting Procedure](#)

[Data Protection Champions' Responsibilities](#)

[Data Protection Impact Assessment \(DPIA\) Screening Questions Checklist and DPIA Template](#)

[Data Protection Glossary](#)

[Data Protection Guidance for Photography and Filming](#)

[Data Protection Lawful Basis Explanations](#)

[Data Protection Policy](#)

[Data Protection Posters – practical actions](#)

[Data Protection Suppression List \(Right to be forgotten\)](#)

[Email Merge from Excel Instructions](#)

[Email Procedures regarding Data Protection](#)

[Guidance for Handling Personal Data Off-Site](#)

[Guidance for Management of Research Data](#)

[Information Classification Table](#)

[Information Security Policy](#)

[Legitimate Interests Assessment \(LIA\) Template](#)

[New Project Development Procedure – Data Protection](#)

[Password Protecting Attachments using 7-Zip](#)

[Privacy Notice Template – How to use it](#)

[Privacy Notice List and Links](#)

[Procedure for Responding to a Data Subject Access Request](#)

[Reviewing Contracts – Data Protection Clauses](#)

[Virus Management Policy](#)

[Wireless Networking Policy](#)