Title:	Data Protection Policy
Policy number:	P075
Policy owner(s):	Data Protection officer
Approval date & version:	March 2025, Ver. 1.2
Approved by:	Academic Board (AB)
Next Review Date:	March 2027

External Reference Points:

External Source	Reference Points
UKQC- Core Practices	N/A
UKQC- Advice and Guidance	N/A
Awarding Body Reference	N/A
Other reference Points Laws, Rules and Regulations	• Data Protection Act 2018 • The EU General Data Protection Regulation 2016
Other Reference Points: NCL Policies	• NCL: Master Information and Security Policy

1. About the Policy

1.1. Background to the General Data Protection Regulation ('GDPR')

The EU General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

From 1 January 2021, the UK is bound by the UK GDPR, which implements the principles of the EU GDPR into domestic law. This works alongside the Data Protection Act 2018 and other relevant laws.

1.2. Definition used by Nelson College London (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (e.g. by computer) and to the processing other than by automated means of personal data (e.g. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the EU GDPR applies to all controllers and processors established in the European Union (EU) that process the personal data of data subjects, in the context of that establishment. It also applies to controllers and processors 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.

The UK GDPR applies to all controllers and processors established in the UK that process personal data. It also applies to controllers and processors outside of the UK that process personal data in order to offer goods and services, or monitor the behaviour of data subjects resident in the UK.

1.3. Article 4 and definitions

Main establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller or processor is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller or processor operates to act on behalf of the controller or processor and deal with supervisory authorities. This term is not used in the UK GDPR.

Personal data – any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Under the UK GDPR, the controller is the organisation that is required to perform the processing under the law. Data subject – any living individual who is the subject of personal data held by an organisation.
Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – 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. There is an obligation on the controller to report

personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent – means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy Statement

2.1. The Board of Directors and management of Nelson College London, located at *106 Olympics House, Clements Road, Ilford, Essex, IG1 1BA* are committed to compliance with the UK GDPR, the Data Protection Act 2018, and all relevant EU and Member State laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information Nelson College London collects and processes in accordance with the GDPR.

2.2. Compliance with the GDPR is described by this policy and other relevant policies such as the Master information security policy, along with connected processes and procedures.

2.3. The GDPR and this policy apply to all of Nelson College London's personal data processing functions, including those performed on students', customers', clients', employees', suppliers' and partners' personal data, and any other personal data the College processes from any source.

2.4. This policy applies to all students, Staff and interested parties of Nelson College London such as outsourced suppliers. Any breach of the GDPR will be dealt with under Nelson College London's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.5. Partners and any third parties working with or for Nelson College London, and that have or may have access to personal data, will be expected to have read and understood this policy, and to comply with it. No third party may access personal data held by Nelson College London without having first entered into a data confidentiality agreement document reference, which imposes on the third-party obligations no less onerous than those to which Nelson College London is committed, and which gives Nelson College London the right to audit compliance with the agreement.

3. Responsibilities and Roles under the GDPR

3.1. Nelson College London is a data controller and/or data processor under the GDPR.

3.2. Top Management and all those in managerial or supervisory roles throughout Nelson College London are responsible for developing and encouraging good information-handling practices within Nelson College London; responsibilities are set out in individual job descriptions.

3.3. The Data Protection Officer/GDPR Owner, a role specified in the GDPR, should be a member of the Senior Management team and is accountable to the Board of Directors of Nelson College London for the management of personal data within Nelson College London and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 Development and implementation of the GDPR as required by this policy; and

3.3.2 Security and risk management in relation to compliance with the policy.

3.4. The Data Protection Officer, whom the Board of Directors considers suitably qualified and experienced, has been appointed to take responsibility for Nelson College London's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Nelson College London complies with the GDPR, as do Manager/Executive (generic/line)'s in respect of data processing that takes place within their area of responsibility.

3.5. The Data Protection Officer/GDPR Owner has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Staff and student seeking clarification on any aspect of data protection compliance.

3.6. Compliance with data protection legislation is the responsibility of all Employees/Staff of Nelson College London who process personal data.

3.7. Nelson College London's staff handbook sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Nelson College London generally.

3.8. Employees/Staff and students of Nelson College London are responsible for ensuring that any personal data about them and supplied by them to Nelson College London is accurate and up to date.

4. Obligations of Research Staff, Students and Research Supervisors

4.1. All staff members involved in carrying out or supervising staff or students responsible for carrying out research that includes the use of personal data must ethical approval is in place and that the research does not cause distress or harm.

4.2. The level of personal data collected should be the minimum amount which is essential for carrying out research and pseudonymisation and anonymisation techniques for data minimisation should be applied.

4.3. Data Protection Impact Assessment is in place if the research is considered high risk.

5. Obligations of Research Staff, Students and Research Supervisors

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Nelson College London's policies and procedures are designed to ensure compliance with the principles.

5.1. Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and
14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

Nelson College London's Privacy policy and procedure are set out at https://nelsoncollege.ac.uk/privacy.

The specific information that must be provided to the data subject must, as a minimum, include:

5.1.1. The identity and the contact details of the controller and, if any, of the controller's representative;
5.1.2. The contact details of the Data Protection Officer;
5.1.3. The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
5.1.4. The period for which the personal data will be stored;
5.1.5. The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
5.1.6. The categories of personal data concerned;
5.1.7. The recipients or categories of recipients of the personal data, where applicable;
5.1.8. Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data; and
5.1.9. Any further information necessary to guarantee fair processing.

5.2. Personal data can only be collected for specific, explicit and legitimate purposes Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the supervisory authority as part of Nelson College London's GDPR register of processing. The https://nelsoncollege.ac.uk/privacy sets out the relevant procedures.

5.3. Personal data must be adequate, relevant and limited to what is necessary for processing.

5.3.1. The Data Protection Officer/GDPR Owner is responsible for ensuring that Nelson College London does not collect information that is not strictly necessary for the purpose for which it is obtained.

5.3.2. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to a privacy statement, and be approved by the Data Protection Officer/GDPR Owner.

5.3.3. The Data Protection Officer/GDPR Owner will ensure that, on an annual basis, all data collection methods are reviewed by internal audit/external experts. to ensure that collected data continues to be adequate, relevant and not excessive.

5.4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay.

5.4.1. Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

5.4.2. The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

5.4.3. It is also the responsibility of the data subject to ensure that the data held by Nelson College London is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

5.4.4. Staff/students/others are required to notify Nelson College London of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained Privacy Procedure It is the responsibility of Nelson College London to ensure that any notification regarding a change of circumstances is recorded and acted upon.

5.4.5. The Data Protection Officer/GDPR Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

5.4.6. On at least an annual basis, they will review the retention dates of all the personal data processed by Nelson College London, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

5.4.7. The Data Protection Officer/GDPR Owner is responsible for responding to requests for rectification from data subjects within one month. This can be extended by a further two months for complex requests. If Nelson College London decides not to comply with the request, the Data Protection Officer/GDPR Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

5.4.8. The Data Protection Officer/GDPR Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

5.5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

5.5.1. Where personal data is retained beyond the processing date, it will be minimised in order to protect the identity of the data subject in the event of a data breach.

5.5.2. Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

5.5.3. The Data Protection Officer/GDPR Owner must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

5.6. Personal data must be processed in a manner that ensures appropriate security.

5.6.1 The Data Protection Officer/GDPR Owner will carry out a risk assessment taking into account all the circumstances of Nelson College London's controlling or processing operations.

5.6.2 In determining appropriateness, the Data Protection Officer/GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Nelson College London itself, and any likely reputational damage including the possible loss of customer trust.

5.6.3 When assessing appropriate technical measures, the Data Protection Officer/GDPR Owner will consider the following:

- Password protection.
- Automatic locking of idle terminals.
- Removal of access rights for USB and other memory media. Virus-checking software and firewalls.
- Role-based access rights including those assigned to temporary staff.
- Encryption of devices that leave Nelson College London's premises such as laptops. Security of local and wide area networks.
- Privacy-enhancing technologies such as pseudonymisation and anonymisation.
- Identifying appropriate international security standards relevant to Nelson College London.

5.6.4 When assessing appropriate organisational measures, the Data Protection Officer/GDPR Owner will consider:

- The appropriate training levels throughout Nelson College London; Measures that consider the reliability of employees (such as references, etc.);
- Including data protection in employment contracts; Identifying disciplinary action measures for data breaches;
- Monitoring staff for compliance with relevant security standards; Physical access controls to electronic and paper-based records; Adopting a clear desk policy;
- Storing paper-based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace; Restricting the use of employee's own personal devices being used in the workplace; Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- and Imposing contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

5.6.5 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

5.6.6 Nelson College London's compliance with this principle is contained in its information security management system (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the Information Security Policy.

5.7. The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

5.7.1. The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

5.7.2. Nelson College London will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, and adopting techniques such as data protection by design, DPIAs, breach notification procedures and incident response plans.

6. Data Subjects' Rights

6.1. Data subjects have the following rights regarding data processing, and the data that is recorded about them:

6.1.1. The right to be informed when their personal data is being processed.

6.1.2. The right to access personal data held about them, including the nature of information held and to whom it has been disclosed.

6.1.3. The right to have processing restricted in certain cases.

6.1.4. The right to prevent processing for purposes of direct marketing.

6.1.5. The right to be informed about the mechanics of automated decision-making processes that will significantly affect them.

6.1.6. The right to not have significant decisions that will affect them made solely by an automated process.

6.1.7. The right to sue for compensation if they suffer damage by any contravention of the GDPR.

6.1.8. The right to have personal data rectified or erased and to block the processing of personal data.

6.1.9. The right to object to processing in specific instances.

6.1.10. The right to request the supervisory authority to assess whether any provision of the GDPR has been contravened.

6.1.11. The right to have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

6.1.12. The right to object to any automated profiling that is occurring without consent.

6.2. Nelson College London ensures that data subjects may exercise these rights:

6.2.1. Data subjects may make data subject access requests (SARs) as described in the Subject Access Request Procedure; this procedure also describes how Nelson College London will ensure that its response to the data access request complies with the requirements of the GDPR.

6.2.2. Data subjects may use data SARs to exercise their other rights.

6.2.3. Data subjects have the right to complain to Nelson College London regarding the processing of their personal data, the handling of data subject requests, and any appeals concerning the outcome of such complaints. These rights shall be exercised in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the College's General Policies and Procedures.

Information about the College's General Policies and Procedures can be found at: https://nelsoncollege.ac.uk/policies-and-procedures

7. Consent

7.1. Nelson College London understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. The data subject can withdraw their consent at any time.

7.2. Nelson College London understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

7.3. There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The controller must be able to demonstrate that consent was obtained for the processing operation.

7.4. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.5. In most instances, consent to process personal and sensitive data is obtained routinely by Nelson College London using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

8. Security of Data

8.1. All Employees/Staff are responsible for ensuring that any personal data that Nelson College London holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Nelson College London to receive that information and has entered into a confidentiality agreement

8.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Master information security policy. All personal data should be treated with the highest security and must be kept:

- If hard copy, in a lockable room with controlled access; and/or If hard copy, in a locked drawer or filing cabinet; and/or
- If electronic, password protected in line with corporate requirements in the Master Information security policy; and/or
- If electronic, stored on (removable) computer media that is encrypted in line with the Master Information security policy

8.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Nelson College London. All Staff and students are required to enter into an Individual User Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

8.4. Hard-copy records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as hard-copy records are no longer required for day-to-day client support, they must be removed from secure archiving in line with procedure reference.

8.5. Personal data may only be deleted or disposed of in line with the Documentation, Retention and Archiving Policy available at: https://nelsoncollege.ac.uk/policies-and-procedures under <General Policies and Procedures>.

8.6. Hard-copy records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by Documentation, Retention and Archiving Policy before disposal.

8.7. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

9. Disclosure of Data

9.1. Nelson College London must ensure that personal data is not disclosed to unauthorised third parties, which include family members, friends, government bodies and, in certain circumstances, the police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with any such risk. It is important to bear in mind whether or not disclosure of the information is relevant to and necessary for the conduct of Nelson College London's business.

9.2. All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer/GDPR Owner.

10. Retention and Disposal of data

10.1. Nelson College London shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

10.2. Nelson College London may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

10.3. The retention period for each category of personal data will be set out in the Documentation, Retention and Archiving Policy available at; https://nelsoncollege.ac.uk/index.php/about/Policies along with the criteria used to determine this period, including any statutory obligations Nelson College London has to retain the data.

10.4. Nelson College London's data retention and data disposal procedures will apply in all cases.

10.5. Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the 'rights and freedoms' of data subjects. Any disposal of data will be done in accordance with the Documentation, Retention and Archiving Policy available at: https://nelsoncollege.ac.uk/policies-and-procedures under <General Policies and Procedures>.

10.6. Under the EU GDPR, all exports of data from within the European Economic Area (EEA) to non-EEA countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

10.7. Under the UK GDPR, all exports of data from within the UK to other countries (third countries) are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

10.8. The transfer of personal data outside of the EEA and or UK is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.8.1. An adequacy decision

- Under the EU GDPR, the European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances, no authorisation is required.
- Countries that are members of the EEA but not of the EU are accepted as having met the conditions for an adequacy decision.
- A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- Under the UK GDPR, the ICO and the Secretary of State for Digital, Culture, Media and Sport can award adequacy decisions to countries that meet the UK's standards for data protection. No authorisation is required for transfers to these countries.
- The UK has awarded adequacy decisions to the EEA and all countries that the EU had awarded adequacy decisions as of 1 January 2021.

10.8.2. Binding corporate rules

- Nelson College London may adopt approved binding corporate rules for the transfer of data. This requires submission to the ICO for approval of the rules that Nelson College London is seeking to rely upon. Binding corporate rules will not be valid if the protections set out in the rules cannot or will not be applied in the recipient state.

10.8.3. Standard contractual clauses

- Nelson College London may adopt approved standard contractual clauses for the transfer of data. If Nelson College London adopts the standard contractual clauses approved by the relevant supervisory authority, there is an automatic recognition of adequacy, provided appropriate measures are taken to ensure the contract clauses can and will be applied within the recipient state.

10.8.4. Exceptions

- In the absence of an adequacy decision, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:
- The data subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subjects request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Compliance With This Policy

All staff and students should make every effort to ensure that they have read and understand this policy. Compliance with this policy's requirements is essential for the safety and security of personal information. If you have any questions or comments, please get in touch with the Data Protection Officer by email at: dataprotectionofficer@nelsoncollege.ac.uk.