NEW COLLEGE LANARKSHIRE

POLCR 16 Data Protection Policy

All College policies and procedures adhere to the guidelines and ethos of Equality and Diversity

When printed, this document becomes

UNCONTROLLED COPY

Always refer to the Intranet to ensure you are accessing the current version

Date of Origin	01/04/2018
Last Updated	26/10/2023
Proposed Review Date	26/10/2025
EQIA Date	23/09/2022
DPIA Date	26/10/2023
Responsibility or Review	College Registrar
Executive Board or Committee Approval	Executive Board

Contents

1 Purpose and Benefits

New College Lanarkshire ("NCL") collects and processes a range of personal data relating to prospective and existingmembers of staff and learners, for a variety of purposes related to employment and the learning experience. We also hold personal data relating to our wider activities and engagement with suppliers and partners.

The lawful and appropriate management of personal data is extremely important to NCL. Our ongoing success depends upon promoting transparency and maintaining the confidence of our learners and staff.

This policy sets out NCL's commitment to protecting personal data and data subject rights, and how it will implement this protection with regards to the handling of personal data as obliged under current data protection legislation.

A failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

2 Scope

This policy applies to all staff employed by the Board of Management of New College Lanarkshire and its provisions extend to all personal data processed by NCL and/or data that is processed on NCL's behalf by a third party.

The policy applies to all personal data, including special category or criminal conviction data held in any format, either digitally or hard copy. It applies to all access to personal data, either on NCL campuses or remotely via home or mobile working.

3 Responsibilities

Overall responsibility for management of information and legislative compliance rests with the **Principal and the Executive Board.**

The **College Registrar** is the designated member of the Executive Board with lead responsibility for data protection.

The **Chief Transformation Officer** has a particular responsibility to ensure the security of all digital systems operated by NCL and the protection of digitally held data.

The **Data Protection Officer** is responsible for NCL's compliance with data protectionlaw and overseeing and updating this policy, and any related policies and procedures as appropriate.

College Deans and **Heads of Academic or Professional Services Departments** are responsible for pursuing the implementationof the policy in their department and ensuring that those processing data in their roles are supported in doing so appropriately.

All College staff have a responsibility to ensure that their actions comply with this policy and operational procedures in their handling and use of personal data, special category data and criminal conviction data.

4 Definitions

For the purposes of this policy, the following definitions, from the UK GDPR (Article 4) apply:

- **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Controller** means 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.
- **Criminal Conviction Data** is the data processed relating to criminal convictions and offences, or related security measures (UK GDPR, Article 10)
- **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.
- **Personal Data** means any information relating to an identified or identifiable natural person ('data subject').
- **Personal Data Breach** means 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.
- **Processing** means 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.
- **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **Special Category 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. (UK GDPR Article 9)

5 The Data Protection Principles

Data protection legislation describes how organisations must collect, handle, and store all personal data, and is underpinned by the following principles.

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

b) 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 (purpose limitation);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will 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 GDPR in order to safeguard the rights and freedoms of data subjects (storage limitation);

f) 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 (integrity and confidentiality).

In addition to these principles the legislation requires organisations to be both responsible for and be able to demonstrate compliance with the above principles (accountability).

NCL will ensure that all data processing for which it is responsible will be conducted in line with these principles and this policy documents how this will be achieved.

6 Lawfulness, Fairness and Transparency

6.1 Lawful basis for processing data

NCL will ensure processing of personal data, meets at least one of the lawful bases as outlined in Article 6 of the UK General Data Protection Regulation (UK GDPR).

Where special category or criminal conviction data is processed, an additional lawful basis will be identified as outlined in Article 9 of the UK GDPR and supported, where relevant, with a condition from Schedule 1 of the Data Protection Act 2018.
Controllers who process special category or personal data relating to criminal convictions and offences under various parts of the Data Protection Act 2018 a required to have an “appropriate policy document”, this document is available in Appendix 1.

At each point that NCL collects data, the lawful basis for processing will be made clear to data subjects via the relevant Privacy Notice.

Where consent or explicit consent is required to process personal data, this consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible format, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the supporting process for Data Subjects to withdraw consent will be simple.

6.2 Privacy Notices (Transparency)

Where NCL collects personal data directly from a data subject, a privacy notice will be made freely

available. The privacy notice will set out the purpose for which the information is being sought, the lawful basis, information on retention of the data, the third parties who NCL may share the data with any relevant international transfers and the data subject rights in relation to this data.

Privacy Notices will be consistent across the college and all notices will be approved by the Data Protection Officer before publication.

Where Personal Data is received by the College from a third party, not the Data subject directly. NCL will provide the Data Subject with all the information required via a Privacy Notice as soon as possible after receiving the data, and no later than one month after receipt.

Where NCL instructs a third party to collect personal data, we will have a contractual relationship, and may require that third party to provide the Data Subject with the information contained in our Privacy Notice on our behalf.

7 Purpose Limitation

Personal data will only be used for the original purpose or purposes for which it was collected. These purposes will be made clear to all data subjects.

Should NCL want to use personal data for a new purpose which was not originally anticipated, this can only proceed under the following conditions. The new purpose is compatible with the original purpose, we collect consent for the new purpose or there is a clear legal obligation requiring the new processing in the public interest. No processing for a new purpose should commence until the relevant privacy notices have been updated and where relevant consent collected.

8 Data Minimisation

NCL will only collect the minimum personal data necessary for the purpose(s) for which it has been collected. Any personal data discovered as excessive or no longer required for the purposes for which it was collected will be securely deleted or destroyed.

Any personal information that is optional for individuals to provide will be clearly marked as such at the point of collection.

9 Accuracy

Where relevant, NCL will take appropriate steps to keep personal data up to date to ensure accuracy and correct processing. The accuracy of personal data will be checked at the point of collection and at appropriate regular intervals afterwards.

Any personal data found or reported to be inaccurate will be updated immediately. Any inaccurate personal data that has been shared with third parties will also be updated.

10 Storage Limitation (Retention)

NCL will retain data for the minimum time necessary to fulfil the purpose(s) for which the data was collected. Where it is no longer necessary to identify individual data subjects, personal data will be anonymised for statistical purposes.

NCL currently refer to the best practice of the JISC Retention Schedules of Further Education in applying relevant retention to records. The JISC retention schedules are published here -Records retention management | Jisc.

NCL has appropriate security measures in place for the deletion and disposal of personal data. Manual records are shredded and disposed of as "confidential waste" and arrangements are in place to permanently erase the hard drives of redundant electronic equipment.

11 Integrity and Confidentiality (Security)

A key principle is that organisations must process personal data securely by means of 'appropriate technical and organisational measures'. NCL is required to ensure the confidentiality, integrity and availability of the systems and services it uses to process personal data.

Accordingly, NCL will implement appropriate security measures to protect personal data throughout its life cycle from collection to destruction. Special category and criminal conviction data will have enhanced security measures.

Personal data will only be accessible to those authorised to access personal data and on a 'need to know' basis.

Members of staff will keep all data secure, by taking sensible precautions and following the NCL ICT Policy Framework, ICT Security Policy and all supporting data protection and information handling related policies and procedures.

12 Accountability

12.1 Appointment of Data Protection Officer

To meet its legal obligations, NCL has appointed a designated data protection officer who is sufficiently independent of operational management and whose duties under data protection arrangements do not pose a conflict of interest with any other duties for which they may be responsible.

12.2 Payment of Fee to ICO as a Data Controller

As required by the Data Protection (Charges and Information) Regulations 2018, NCL pay an annual fee to the Information Commissioners Officer (ICO). Our registration number is Z9194349 and register entry is available to view on the ICO website.

12.3 Record of Processing Activities

NCL will maintain a Record of Processing Activities that documents all processing activities for which it is responsible.

The Record of Processing Activities will hold details of each processing activity including the purpose of processing; categories of data and data subject; lawful basis, any additional conditions for special category or criminal conviction data; third party recipients; retention and relevant technical and organisational security measures. This will be reviewed on a regular basis.

12.4 Data Processors

Where NCL engages Data Processors to process personal data on its behalf, we will ensure an

appropriate level of due diligence is completed in relation to the risk of the processing activity and appropriate legally binding contract or agreement is in place. The contract or agreement will detail all obligations of both NCL as a Data Controller and the third party as a Data Processor in accordance with UK GDPR Article 28.

12.5 Data Protection by Design

NCL has an obligation to implement technical and organisational measures to demonstrate that it has considered and integrated data protection into all of its processing activities. This ensures that good data protection practice is embedded in all NCL activities from the start and that appropriate data protection safeguards are part of all development and design specifications, as part of a 'privacy first' approach.

12.6 Data Protection Impact Assessments

In designing and operating systems and processes, or when introducing any new type of processing (particularly using new technologies), NCL will carry out a Data Protection Impact Assessment (DPIA)to consider whether the proposed processing activity is likely to result in a high risk to the rights and freedoms of individuals and to identify appropriate safeguards or alternative approaches.

Where NCL proposes to introduce or amend new systems or working practices that include processing personal data, an initial data protection impact screening assessment will be undertaken to assess if there is a requirement to conduct a full DPIA.

NCL will manage risk and consider what control measures are appropriate to ensure that data remains protected and all processing remains compliant with the principles set out above. No processing of personal data will be undertaken where high risks have not been appropriately mitigated during the DPIA process.

13 Data Subject Rights

NCL will uphold the rights of data subjects to access and retain control over their personal data processed. Data Subjects have the following rights:

- **Right to be Informed** – by ensuring data subjects are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that data subjects are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. NCL will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (also known as 'the right to be forgotten') – NCL will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** – NCL will restrict processing when a valid request is received by a data subject and inform data subjects of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine readable format.

- **Right to Object** – by stopping processing personal data, unless NCL can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defense of legal claims.

These rights may be qualified, limited or modified by the lawful basis on which data is processed.

Where staff receive a communication from any individual which seeks (or might be construed as seeking) to exercise any rights in relation to Personal Data this must be notified to the Data Protection Officer and managed under the Data Subject Rights Procedures.

14 Data Sharing

In the performance of its duties in relation to the employment and the services provided to learners, the College will share personal data with third parties. This may be part of a regular exchange of data, or one-off disclosures in unexpected or emergency situations. Any regular data sharing will be included in the appropriate Privacy Notices.

Appropriate security measures and safeguards will be used when sharing any personal data externally. In all cases, NCL will consider all the legal implications of sharing personal data prior to doing so.

14.1 Regular Data Sharing

Where data is shared regularly a contract or data sharing agreement will be in place to establish what data will be shared, agreed purpose and security arrangements. A register of all such data sharing agreements will be kept by the NCL's Data Protection Officer.

Any contract or agreement to which NCL is party that relates to data sharing, access to NCL data or processing activities will be reviewed by the Data Protection Officer prior to signature by the relevant NCL representative.

14.2 Disclosure to Police and other Government Agencies

There may be requests made to NCL to share data with the Police, law enforcement agencies or other bodies with statutory functions to detect or prevent crime. These requests will be handled under the Requests for Personal Data from Police and other Gov Agencies Procedures and careful consideration taken on the application of any exemptions to disclosure data.

All decisions to disclose personal data to these agencies will be approved by a member of the Executive Board, with the exception of emergency situations where a delay in approval would cause a risk of harm to an individual.

14.3 Disclosure to Third Parties

NCL must ensure that personal data is not disclosed to unauthorised third parties which includes family members. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

Personal data will only be disclosed where NCL has a lawful basis for this disclosure. Where appropriate, the data subject may be asked to provide consent to the disclosure.

If there is any doubt as to whether it is legitimate or otherwise to disclose personal data to a third party, staff should seek advice from their line manager who will consult with a member of the Executive Board or the NCL Data Protection Officer, as necessary.

15 International Transfer

The UK GDPR imposes restrictions on the transfer of personal data outside the UK. Personal data may only be transferred outside the UK when there are safeguards in place to ensure an adequate level of protection for the data.

NCL will only transfer personal data outside the UK when:

- the receiver is located in a third country covered by UK adequacy regulations; or
- appropriate safeguards are in place, such as Standard Contractual Clauses; or
- the transfer covered by an exception.

Staff involved in transferring personal data to other countries must consult the Data Protection Officer prior to doing so and ensure that appropriate safeguards are in place before agreeing to any such transfer.

16 Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. NCL has procedures in place to contain, mitigate, manage and notify a personal data breach.

For any personal data breaches, the Data Protection Officer and College Registrar will be responsible for developing an appropriate Breach Management Plan in accordance with the Personal Data Breach Management Procedures.

Where there is a risk identified to the rights and freedoms of individuals, UK GDPR makes notification of a breach to the Information Commissioner's Office mandatory, and notification must take place within 72 hours of an organisation becoming aware of the breach. It is therefore essential that any breaches, or suspected breaches, within NCL or in relation to NCL data are reported to the Data Protection Officer promptly, to enable appropriate investigation, containment and risk assessment to be undertaken.

Decisions to notify the Information Commissioner's Office, the individuals affected and any relevant third parties will be taken promptly, if required. All notifications will be coordinated by the Data Protection Officer or College Registrar.

16.1 Breach of this policy

While the purpose of this policy is to ensure that NCL's data protection arrangements are effective and well understood, it is also important to recognize the behaviours and actions that would be considered as breaches of the policy and the consequences of any such breach. The following occurrences are considered breaches of this policy:

- Unlawful procurement of information by anyone not entitled to access such information.
- Unfair processing i.e., processing information for a purpose other than that for which it wasprovided.

- Processing of inaccurate information, particularly if information was known to be inaccurate or steps could have been taken to ensure accuracy.
- Unlawful disclosure i.e., sharing of information with anyone not entitled to receive it or loss ofany data subject to this policy.
- Collection, storage or processing of inadequate, irrelevant or excessive information.

Unlawful disclosure, inadequate/irrelevant/excessive information are all breaches of this policy. Any abuses of this policy by a member of staff may result in action taken in accordance with the Staff Disciplinary Policy and Procedure.

17 Staff Training and Awareness

All staff will be made aware of good practice in Data Protection and where to find guidance and support for data protection issues. Further information on NCL procedures for handing personal data are also included within other relevant policies and procedures listed in Section 18.

Adequate and role specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities. Additional specialist training given to staff in areas with specific responsibilities for processing special category or criminal conviction data. Completion of initial and refresher training in data protection will be mandatory for all staff.

Individual members of staff required to handle sensitive data in the course of their employment at the College will have a confidentiality clause contained within their Written Terms andParticulars of Employment, which will explicitly state that unauthorised disclosure or a breach of the Data Protection Policy may result in disciplinary action.

18 Related Policies and Procedures

This policy is supported by the following policies and procedures:

- PROCR 16.1 Information Security Incident Procedures
- PROCR 16.2 DPIA Procedures
- PROCR 16.3 Data Subject Rights Procedures
- ICT Policy Framework
- ICT Security Policy

All of these documents can be accessed via Data Protection section of The Clan.

19 Monitoring and Review

New College Lanarkshire will review its practices and provisions on a regular basis to ensure that they reflect our commitment to ensuring fair, consistent and lawful management of data.

The policy will be reviewed bi-annually or in response to any significant change in practice or legislation to reflect legislative requirements, recommendations and identified good practice.

Appendix 1

Appropriate Policy Document

As part of NCL's data processing activities we will process special category data and criminal offence data under Article 9 and 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018. The Data Protection Act 2018 requires an Appropriate Policy Document under Schedule 1, Part 4.

This Appropriate Policy Document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. It also supplements the information provided in the main Data Protection Policy, the Record of Processing Activities and Privacy Notices.

1. Compliance with Principles

NCL complies with the UK GDPR Article 5 principles, as outlined in the Data Protection Policy, Sections 5 - 12.

2. Processing activities and conditions

NCL maintain a Record of Processing Activities that documents all processing. NCL relies on the following UK GDPR Article 9 lawful basis and DPA2018 Schedule 1 conditions to process special categories of personal data:

2.1 Employment, social security and social protection purposes (UK GDPR Article 9(2)(b))

- Part 1, 2. Health and Social care purposes (b) assessment of the working capacity of an employee.
- Part 2, 11 protecting the public against dishonesty etc. (2)(a) – protect members of the public against dishonesty, malpractice, or other seriously improper conduct.
- Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law.

Example of this processing include staff sickness and absence management, disciplinary and grievance procedures, trade union membership.

2.2 Health or social care (UK GDPR Article 9(2)(h))

- Part 1, 2. Health and Social Care purposes (a) occupational medicine and (b) assessment of working capacity of an employee

Example of this processing include Occupational Health records.

2.3 Reasons of substantial public interest (UK GDPR Article 9(2)(g))

- Part 2, 8. (1) – equality or opportunity of treatment
- Part 2, 6. (2)(a) – exercise of a function conferred by an enactment or rule of law
- Part 2, (16) – support for individuals with a particular disability or medical condition
- Part 2, (18) Safeguarding of children and of individuals at risk

Examples of this processing includes equality monitoring and reporting, protected disclosures, development of personal learning support plans, personal emergency evacuation plans and safeguarding.

This also includes criminal offence data where NCL has a statutory duty to protect children and vulnerable adults, as outlined in the Protection of Vulnerable Groups (Scotland) Act 2007. Under this

legislation NCL will conduct criminal conviction checks to ensure that its staff or students undertaking regulated work do not pose a threat to the safety of children and vulnerable adults.

2.4 Other Special Category Processing

NCL processes special category personal data in other instances where it is not a requirement to keep an Appropriate Policy Document. We provide clear and transparent information about why we process personal data including our lawful basis in our relevant privacy notices.

3. Retention and Erasure Policies

All special category and criminal offence data are retained in line with our Data Protection Policy, Section 10 - Storage Limitation (Retention)

4. Appropriate Policy Document Review

This document will be reviewed bi-annually or updated as necessary where processing activities change.

Version Control

Date	Page Number/Paragraph/ Section/Form	Description of Change	Rationale for Change
March 2023	Title	Re-coded to align with new Policy Management Procedure	To ensure coded correctly on policy register
October 2023	1. Section 18 Related Policies and Procedures 2. Appropriate Policy Document, Section 4. 3. Version Control section added	1. Titles of related procedures updated to include correct coding. 2. To align review date with main policy. 3. To align with Policy Management Procedures	Bi-annual review