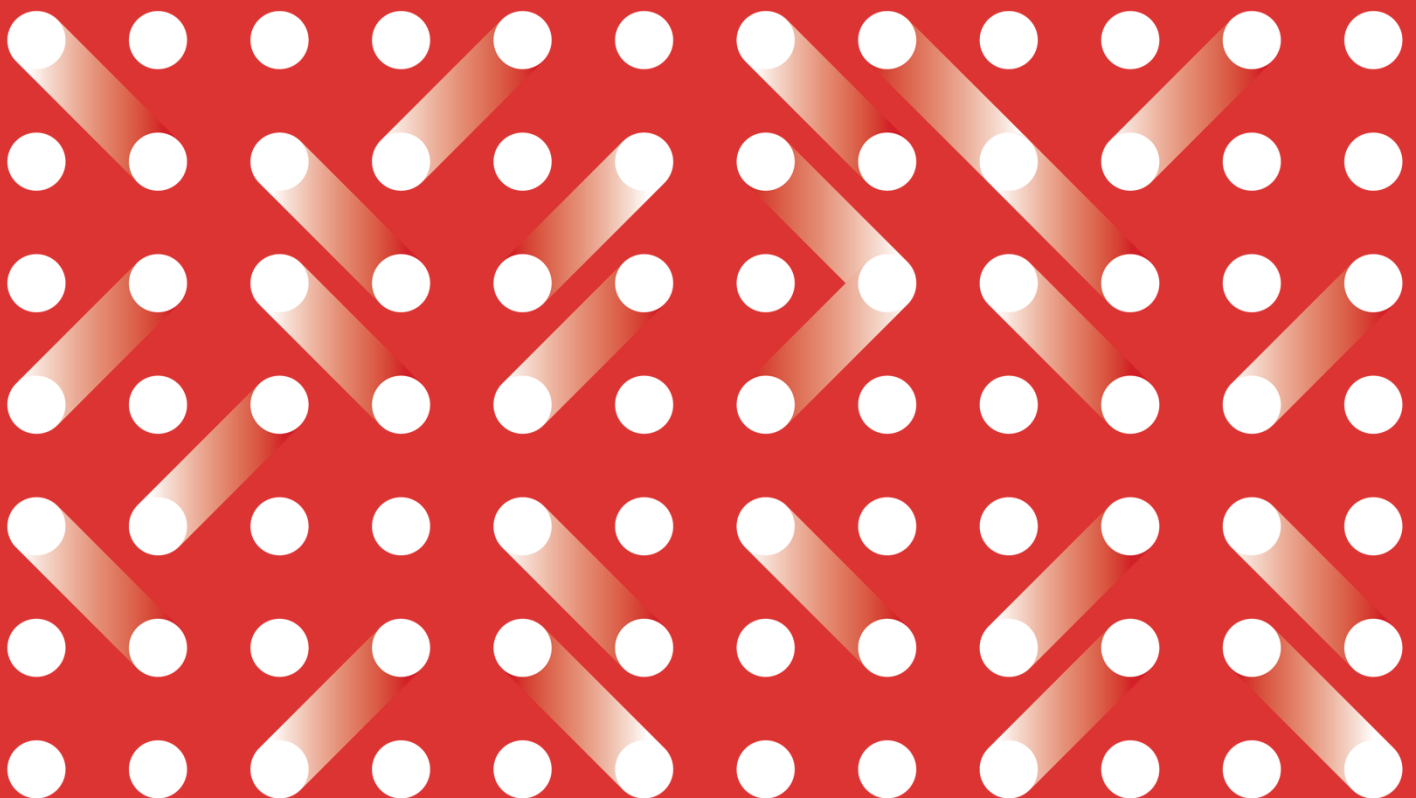


Privacy Policy



Contents

VERSION 3.3.....	2
POLICY OVERVIEW	3
PRIVACY POLICY	5
Personal Data	6
Processing.....	7
Identity and Contact Information.....	7
Education and Employment Information	8
Compliance Information.....	8
Financial Information.....	8
Technical and Usage Data	8
Special Category Data (if applicable)	8
Information You Provide Directly.....	9
Information Collected Automatically.....	9
Information Obtained from Third Parties	9
Security Measures	14
User Responsibilities.....	15
Incident Identification and Reporting	15
Breach Investigation and Containment.....	15
Notification and Communication.....	15
Remediation and Prevention.....	16
SUPPORTING DOCUMENTS	17
MONITORING	17

Version 3.3

<i>Release Date</i>	<i>Version No.</i>	<i>Summary of Main Changes</i>	<i>Owner</i>
September 2021	2.1	Policy (legacy)	NCUK Director of Digital
December 2024	3.0	New Policy Created	CIO/Head of Technology
January 2025	3.1	SME Review and comments	CIO/Head of Technology
July 2025	3.2	Published	CIO/Head of Technology
August 2026	3.3	Connect, student lawful basis, marketing, data-sharing and 2026 legal updates	Legal Team

Policy Overview

Why do we have this policy?

The purpose of this document is to provide information on how NCUK collects, processes, and manages personal data in accordance with applicable laws and regulations, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The intention of this document is not to impose restrictions that are contrary to a culture of openness, trust, and integrity but to ensure compliance with legal and regulatory obligations. This policy aims to protect the privacy of individuals, including students, employees, and third parties, and to uphold NCUK's commitment to responsible data handling.

This policy is intended to be a statement of high-level data protection requirements that must be met. It is unlikely that exceptions to this policy will be required; however, if an activity does require an exception, it must be approved by the Data Protection Officer (DPO), Chief Information Officer, or Chief Financial Officer and tracked using the risk management framework.

Similarly, if you become aware of any aspect of personal data processing within NCUK that does not adhere to this policy, it must be reported and managed using the risk management framework.

Who does this policy apply to?

This policy applies to both NCUK staff responsible for implementing data protection measures (employees, contractors, consultants, and temporary staff) and individuals whose data is managed by NCUK.

NCUK works with Study Centres, NCUK Partner Universities and vendors when delivering its services. Their data protection roles differ by activity: some organisations process personal data on NCUK's instructions, while others decide their own purposes and act as independent or joint controllers.

This policy applies to all personal data collected, stored, processed, or transmitted by NCUK, regardless of format or location. It covers all digital and physical records, including student and staff data, financial information, and system logs.

This policy applies unless an alternative contractual clause or privacy policy is in place, such as a supplier contract or contract of employment, which explicitly governs the handling of personal data.

Compliance with NCUK's policies is mandatory. Non-compliance could have a significant effect on the efficient operation of our business and may result in financial loss and/or an inability to provide necessary services to our clients. If any employee is found to have breached any organisational data protection policies, they may be subject to the disciplinary process.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your immediate manager or the Data Protection Officer (DPO).

Privacy Notice

Introduction

Northern Consortium UK Limited (company number 04842064), trading as NCUK, is committed to protecting your privacy and handling personal data fairly, transparently and lawfully. This Privacy Notice reflects the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and, where relevant, the Privacy and Electronic Communications Regulations 2003 (PECR).

This Privacy Notice explains what personal data we collect, where it comes from, how and why we use it, who we share it with, how long we keep it, and your data protection rights.

NCUK is a controller where we decide why and how your personal data is used. Study Centres, NCUK Partner Universities and other organisations may also act as separate controllers for their own purposes. Where another organisation processes personal data only on NCUK's instructions, it acts as our processor.

For any privacy-related inquiries, please contact our Data Protection Officer (DPO):

By email dpo@ncuk.ac.uk

or write to.

Data Protection Officer, NCUK

Spaces Peter House
Oxford Street
Manchester
M1 5AN

Students and the Connect platform

If you are an NCUK student, your Study Centre will usually register you with NCUK and provide us with information about you before you first log in to Connect. This may include your name, date of birth, contact details, identification information, programme details, entry qualifications and other information needed to register and support you.

Core student processing

We use core student information to create and maintain your NCUK record; administer your qualification, assessments, academic progress, results and certificate; operate Connect and other student systems; send important service communications; protect academic standards and system security; and, where applicable, support your progression and applications to NCUK Partner Universities.

For this core processing, our principal lawful basis is Article 6(1)(f) UK GDPR (legitimate interests), rather than consent. Our legitimate interests are delivering and administering NCUK qualifications and student services, maintaining accurate academic records, supporting progression to university, protecting academic integrity, and operating secure and effective systems. NCUK has documented this assessment in a Legitimate Interests Assessment.

Many NCUK students are under 18. We give particular weight to children's rights and interests, use age-appropriate explanations, limit processing to what is needed, and apply appropriate security and access controls. Being under 18 does not, by itself, mean that parental consent is required for this core processing because consent is not the lawful basis on which we rely.

Core service communications

We will send communications that are necessary to administer your NCUK programme and support your university progression, such as registration, assessment, results, application actions, deadlines, offers and important service updates. These service communications are separate from promotional marketing. Email is normally the main service channel; where Connect offers additional service channels such as SMS, WhatsApp or telephone, you may be able to set channel preferences.

Marketing choices

Promotional marketing is optional. Where consent is required, we will only send marketing through a channel that you have positively chosen to opt in to. Marketing options will not be pre-selected for you. You can change your marketing choices or withdraw consent at any time, and doing so will not affect your NCUK qualification, assessments, results, certificate, Connect access or core university application support.

Optional external providers

From time to time, NCUK may offer optional services from external providers, such as accommodation or other student-support services. Where sharing your personal data with an independent external provider is optional and relies on consent, we will identify the provider and explain the purpose of the sharing before you opt in. This is different from sharing that is necessary to deliver NCUK's core services, such as sharing with NCUK service providers, your Study Centre or an NCUK Partner University in connection with an application.

Key Definitions

Personal Data

Personal data refers to any information relating to an identified or identifiable individual. This includes, but is not limited to:

- Contact details (name, address, email, phone number)
- Identification numbers (e.g., student ID, passport number)
- Personal characteristics (e.g., date of birth, gender, nationality)
- Photographs and biometric data
- Records of communications or interactions with NCUK
- Expressions of opinion about the individual or indications of NCUK's intentions toward them

Processing

Processing refers to any operation or set of operations performed on personal data, whether automated or manual. This includes, but is not limited to:

- Collecting, recording, organising, and structuring
- Storing, adapting, or altering
- Retrieving, accessing, consulting, and using
- Disclosing, disseminating, or otherwise making available
- Aligning, combining, restricting, erasing, or destroying

Terms used in this Privacy Notice

- **Adequacy Decision:** means that the relevant country has been recognised as having an appropriate legal framework for protection of personal data.
- **Clearing:** means the process by which universities offer places they have not yet filled to applicants who do not hold an offer.
- **EEA:** means the countries of the European Economic Area from time to time.
- **NCUK Partner Universities** means the universities NCUK works with to provide progression routes for students, a full list of which can be viewed on the NCUK website at <https://www.ncuk.ac.uk/universities/>
- **Study Centre** means one of our approved centres for studying for an NCUK qualification.
- **UCAS Portal:** means the centralised admission process for UK universities operated by the Universities Centralised Admissions Service at www.ucas.com

The Data We Collect

We collect and process various types of personal data, including information from students, employees, study centre personnel, contractors, and other third parties who engage with NCUK. The categories of personal data include:

Identity and Contact Information

- Name, date of birth, gender

- Contact details (address, email, phone number)
- Emergency contact details

Education and Employment Information

- Academic history, qualifications, certifications
- English language test scores
- CVs, employment history, and references (for employees, study centre personnel, and contractors)

Compliance Information

- Visa and immigration status
- Passport and ID numbers
- Right-to-work documentation

Financial Information

- Payment details

Technical and Usage Data

- IP address, browser type, and device information
- Online engagement (cookies and analytics tracking)
- Access logs and system activity for users accessing NCUK systems

Special Category Data (if applicable)

- Health or disability information (for accommodation and support needs)
- Racial or ethnic origin (for statistical and diversity monitoring)

Criminal Offence Data (if applicable)

Where NCUK actually receives or handles criminal offence information, this may include DBS check information or information about criminal convictions, offences or allegations where this is necessary and lawful for employment, safeguarding or relevant university/visa requirements.

Criminal offence data is subject to additional protections under Article 10 UK GDPR and the Data Protection Act 2018. NCUK will identify an Article 6 lawful basis and an applicable Schedule 1 condition before processing it, and will maintain an Appropriate Policy Document where the law requires one. NCUK does not rely on employee consent alone as the basis for required DBS or safeguarding processing.

How we collect your data

We gather personal data through various methods, which include:

Information You Provide Directly

You may share your personal information with us through various interactions, such as:

- Completing application forms, either online or in physical format
- Submitting a CV, job application, or employment documentation (for employees, contractors, and study centre personnel)
- Signing a contract of employment, supplier contract, or partnership agreement
- Registering to access NCUK systems, including learning platforms and administrative portals
- Contacting us via email, phone, post, or other communication channels
- Applying for a place on a course or making an enquiry
- Confirming acceptance of a study place
- Requesting promotional materials or subscribing to updates
- Participating in surveys or providing feedback

Information Collected Automatically

When engaging with our websites and digital services, we may automatically collect certain technical details, including:

- Device and browser specifications
- Browsing patterns and site interactions
- IP addresses and system logs

This data is gathered using cookies and other tracking technologies. For additional details, please refer to our Cookies Policy.

Information Obtained from Third Parties

In some cases, we receive personal information from trusted third parties, such as:

- Analytics and search service providers supplying technical data on website usage
- Payment processors managing financial transactions on our behalf
- Study Centres, education counsellors and NCUK Partner Universities assisting with registration, qualification administration, applications, admissions or progression
- Parents or guardians where relevant, including where information is needed in connection with an under-18 student, safeguarding, welfare or university enrolment requirements
- Regulatory bodies (e.g., UK Visas and Immigration) providing compliance-related data

This data is handled in accordance with applicable privacy laws and contractual obligations to ensure its lawful and secure use.

How we use your data

We process your data for the following purposes:

- To register students, create and maintain NCUK student records, and administer NCUK qualifications
- To administer assessments, academic progress, results, certificates and related academic and student support
- To provide university progression and application support in relation to NCUK Partner Universities, where applicable
- To comply with legal obligations (e.g., immigration requirements)
- To manage financial transactions and payments
- To send essential programme and progression communications and, separately, optional marketing where you have opted in
- To operate Connect and other NCUK digital services, including account administration, audit logs and service improvement
- To ensure IT security and fraud prevention

Legal Basis for Processing

Our legal bases for processing personal data include:

- **Contract (Article 6(1)(b)):** where processing is necessary for a direct contract with you, for example the NCUK Student Terms and Conditions where applicable, or an employment or supplier contract
- **Legal obligation (Article 6(1)(c)):** where processing is necessary for NCUK to comply with a legal obligation
- **Legitimate interests (Article 6(1)(f)):** including the core student processing described above, academic administration and integrity, university progression support, quality assurance, fraud prevention, IT and information security, and the effective operation of NCUK's services. When we rely on this basis, we consider necessity, reasonable expectations and the impact on your rights, with particular care where students are under 18
- **Consent (Article 6(1)(a)):** where you make a genuinely optional choice, including electronic marketing where consent is required and optional sharing with a named external provider. You can withdraw consent at any time
- **Vital interests (Article 6(1)(d)):** where processing is necessary to protect someone's life in an emergency.

Where we process special category data, we must also identify a condition under Article 9 UK GDPR. Where we process criminal offence data, Article 10 UK GDPR and an applicable condition in Schedule 1 of the Data Protection Act 2018 also apply. We use these categories only where necessary and with additional safeguards.

Data sharing and transfers

We may share your personal data with:

- NCUK Partner Universities where this is necessary to support an NCUK application or progression route, provide relevant academic information, manage offers/admissions or confirm enrolment. If you choose to apply independently to a non-partner university, NCUK does not normally share your data with or provide application support to that university unless this is separately agreed.
- Study Centres or Test Centres where this is necessary to administer your enquiry, registration, programme, assessment, qualification, progression or support. International transfers are dealt with separately below.
- UK government bodies where we have a legal obligation to do so.
- Professional and Legal Service Providers Including auditors, legal advisors, and HR or payroll service providers.
- Your parent or guardian in an emergency, where your health or welfare requires it.
- Independent quality assessors for the purposes of assuring the quality of our services.
- Our corporate service providers as part of the business services they provide to us, subject to strict obligations of confidentiality.
- Payment Processors and Financial Institutions to manage payments, payroll, and supplier transactions.
- Third-Party IT and Cloud Service Providers who support NCUK's systems, including learning platforms, CRM, and HR systems.
- Optional external service providers where you have actively opted in to a specific service and data sharing is based on your consent. We will identify the provider and purpose before the sharing takes place.

The information we collect from you may be transferred to, and stored at, destinations outside the United Kingdom (UK). It may also be processed by staff operating outside the UK who work for us, another NCUK entity, or one of our suppliers..

Where personal data is transferred outside the UK in a way that constitutes a restricted transfer, NCUK does not rely on the fact that you submitted the data as permission for the transfer. We use a lawful transfer mechanism and, where required, assess the risks of the transfer. Safeguards may include:

- We transfer your personal data to countries deemed by the UK government to provide an adequate level of protection, as specified in 'adequacy regulations'.
- We use appropriate contractual safeguards where required, such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, together with any required transfer risk assessment. You can

contact dpo@ncuk.ac.uk for further information about the safeguards used for a particular transfer.

Data Retention

NCUK will only retain personal data for as long as necessary to fulfil the purposes for which it was collected, including to satisfy legal, accounting, or reporting obligations.

To determine the appropriate retention period for personal data, we consider several factors, including:

- The volume, nature, and sensitivity of the data.
- The potential risk of harm from unauthorised use or disclosure.
- The purpose for processing the data and whether those purposes can be achieved through other means.
- Applicable legal and regulatory requirements.

Certain core academic award records may be retained for a long period, and where necessary indefinitely, so that NCUK can verify qualifications and provide replacement transcripts or certificates. This does not mean that every item in a student's Connect or CRM record is retained indefinitely; other information is retained only for as long as needed for its specific purpose.

After the relevant retention period has expired, NCUK will securely delete or anonymise personal data to ensure it cannot be linked back to an individual. In cases where anonymisation is not possible, data will be securely destroyed in accordance with NCUK's data disposal policies.

Individuals may request further information on specific retention periods by contacting the Data Protection Officer at dpo@ncuk.ac.uk

If you choose not to provide personal information?

Some personal data is necessary for NCUK to register you, administer your qualification, assessment and award, operate student systems, or provide an agreed service. Depending on the activity, we may rely on legitimate interests, contract or legal obligation rather than consent. If essential information is not provided, we may be unable to provide or continue the relevant service.

In such cases, we may need to cancel your requested service, but we will notify you if this is necessary at the time of the request.

Failure to provide essential personal data may also impact our ability to comply with regulatory obligations or fulfil commitments related to your education, assessment, certification, or support services.

Automated decision-making

Connect and other NCUK systems may automate routine workflows, reminders and administrative steps. NCUK does not currently use Connect to make decisions about students based solely on automated processing that produce legal or similarly significant effects. If this changes, we will provide the additional information required by data protection law.

Your rights

Under data protection law, you have several rights concerning the processing of your personal data. These rights include:

- **Right to Access:** You have the right to request a copy of the personal data we hold about you, commonly known as a "data subject access request," to check its accuracy and ensure it is being processed lawfully.
- **Right to Rectification:** If any personal data we hold about you is incorrect or incomplete, you can request that we update or correct it. Verification of the new data may be required before changes are made.
- **Right to Erasure:** You can ask us to delete or remove your personal data where there is no valid reason for us to continue processing it. This also applies where you have exercised your right to object, where we have processed data unlawfully, or where legal obligations require us to erase your information. However, in some circumstances, we may be unable to comply with your request for legal or operational reasons, which will be communicated to you.
- **Right to Object:** Where we rely on legitimate interests, you can object to the processing. We will consider your circumstances and stop the processing unless we can demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing is needed for legal claims. You have an absolute right to object to direct marketing.
- **Right to Restrict Processing:** You may request that we suspend the processing of your personal data in specific scenarios, including when verifying its accuracy, if our processing is unlawful, if you require the data to establish or defend legal claims, or if you have objected to our use of the data but verification of overriding legitimate interests is required.
- **Right to Data Portability:** You can request that we provide your personal data to you or to a third party in a structured, commonly used, machine-readable format. This

applies only to automated data that you provided to us with consent or as part of a contract.

- **Right to Withdraw Consent:** If we rely on your consent, you may withdraw it at any time. This will not affect processing that was lawful before withdrawal. Withdrawing marketing or optional external-provider consent will not stop the core student processing that NCUK carries out on another lawful basis.

You can change your marketing choices through the communication preferences made available to you, use the unsubscribe option in a promotional message, or contact us directly. A marketing opt-out does not stop essential programme or progression communications.

If you wish to exercise any of the rights listed above or require further information, please contact us at dpo@ncuk.ac.uk. To process your request securely, we may require additional information to confirm your identity. We may also contact you for further details to expedite our response.

We aim to respond to all legitimate requests as soon as possible and within one calendar month. If your request is complex or if multiple requests have been made, it may take longer, but we will notify you and keep you updated on progress.

Data protection complaints

If you think NCUK has not handled your personal data properly, you can make a data protection complaint by contacting dpo@ncuk.ac.uk. We will acknowledge a complaint within 30 days, take appropriate steps to investigate it without undue delay, keep you informed where appropriate, and tell you the outcome.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority. Further information is available at www.ico.org.uk/make-a-complaint or by telephone on 0303 123 1113.

Information Security

NCUK places significant emphasis on the security of personal data and employs a combination of technological, physical, and organisational measures to prevent unauthorised access, unlawful processing, accidental loss, alteration, disclosure, destruction, or damage.

Security Measures

We implement procedures and technologies to maintain data security throughout its lifecycle, from collection to disposal. We ensure that:

- Personal data is protected against unauthorised access through encryption, access controls, and secure storage solutions.
- Organisational policies govern data access, ensuring that only authorised personnel handle sensitive information.
- Data is transferred to third parties only if they comply with equivalent security standards or establish adequate protective measures.

User Responsibilities

Users must take responsibility for safeguarding their login credentials and personal information. Specifically:

- Any passwords issued for accessing our websites or virtual learning environments must remain confidential.
- Users must not share their passwords with others.
- NCUK is not liable for unauthorised transactions resulting from compromised credentials.

For additional guidance on maintaining security, please refer to NCUK's Information Security Policy.

Data Breach Response

NCUK takes data security and privacy seriously and has established procedures to respond effectively to security incidents and data breaches.

Incident Identification and Reporting

All employees, contractors, and third parties with access to personal data must report any suspected or actual data breach immediately to the Data Protection Officer (DPO) at dpo@ncuk.ac.uk

Breach Investigation and Containment

Upon receiving a report, NCUK will:

- Assess the nature and scope of the breach.

Take immediate steps to contain and mitigate risks associated with the breach.

- Engage relevant stakeholders, including IT security teams, legal advisors, and management.

Notification and Communication

If a personal data breach is likely to result in a risk to people's rights and freedoms, NCUK will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible,

within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk to affected individuals, NCUK will also inform those individuals without undue delay.

Where applicable, NCUK will also inform affected individuals about:

- The nature of the breach.
- The steps taken to mitigate risks.
- Guidance on what they should do to protect themselves.

Remediation and Prevention

Following a data breach, NCUK will:

- Conduct a post-incident review to identify the root cause.
- Implement necessary changes to policies, processes, or security measures to prevent recurrence.
- Provide additional training to staff if required.

For more details on how NCUK handles data breaches, refer to the Security Incident & Data Breach Response Policy or contact the Data Protection Officer.

Changes to this privacy notice

We reserve the right to update this Privacy Notice at any time, the most recent version can be viewed on our website at <https://www.ncuk.ac.uk/ncuk-policies/>. We may also notify you in other ways from time to time about the processing of your personal information.

Supporting documents

NCUK has developed several supporting policies, standards, frameworks, and guidelines to accompany this policy document.

Other supporting policies are listed below:

- Information Security Policy
- Data Retention Policy
- Security Incident & Data Breach Response Policy

Monitoring

This policy shall be reviewed at least once a year or earlier if changes in the business environment may impact its content. The review shall assess the impact of changes in information assets, deployed technology, and legal or regulatory requirements. The NCUK Legal and Compliance Team shall approve significant changes to this policy and communicate them to all interested parties, ensuring its effectiveness and relevance.

Review Arrangements

This document will be reviewed annually as part of the NCUK self-evaluation arrangements. It may also be revised as and when necessary, in response to feedback, trends from our internal monitoring arrangements, changes in our practices, actions from the regulatory authorities (where applicable) or external agencies or changes in legislation.

If you would like to feedback your views, please contact quality@ncuk.ac.uk

Spaces Peter House
Oxford Street
Manchester
M1 5AN
United Kingdom

Tel: 0161 549 9220

www.ncuk.ac.uk

NCUK
UNIVERSITY PATHWAYS