NCIUL Data Protection Policy

GDPR-2018

ADM-DPP 103

Contents

Introduction

NCIUL needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example.

It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, NCIUL must comply with the Data Protection Principles, which are set out in the GDPR 2018 and Data Protection Act 1998.

In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Compliance with the GDPR 2018 and Data Protection Act 1998 is the responsibility of all members of NCIUL. NCIUL and all staff or others who process or use any personal information must ensure that they follow these principles at all times. Any deliberate breach of the data protection policy may lead to disciplinary action being taken or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Human Resources.

Responsibilities of staff

All staff are responsible for:

- Checking that any information that they provide NCIUL in connection with their employment is accurate and up to date.
- Informing NCIUL of any changes to information, which they have provided, eg changes of address.
- Informing NCIUL of any errors or changes in staff information. NCIUL cannot be held responsible for any such errors unless the staff member has informed NCIUL of them.
- If and when, as part of their responsibilities, staff collect information about other people, (e.g. about students' coursework, opinions about ability, references from other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff (Appendix 1).

Data security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely, for example, kept in a locked filing cabinet; or in a locked drawer; if it is computerised, be password protected; or kept only on disk, which is itself kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

Student obligations

Students must ensure that all personal data provided to NCIUL is accurate and up to date. They must ensure that changes of address and contact details are notified to the Registrar.

Rights to access information

Staff, students and other users of NCIUL have the right to access any personal data that is being kept about them either on computer or in hard copy. Any member of staff who wishes to exercise this right should contact the Human Resources Office. Students should contact the Student Office.

In order to gain access, an individual may wish to receive confirmation of the information currently being held. This request should be made in writing. NCIUL will make a charge on each occasion that access is requested. NCIUL aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days.

If an individual makes a complaint or is otherwise dissatisfied with the way their personal information is being processed by NCIUL, they should contact the Human Resources Office.

Subject consent

In many cases, NCIUL can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to NCIUL processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974.

NCIUL has a duty of care to all staff and students and must therefore make sure that employees and those who use NCIUL facilities do not pose a threat or danger to other users. Therefore, all prospective staff and students will be asked to consent to their

data being processed when an offer of employment or a course place is made. A refusal to sign such a form may result in the offer being withdrawn.

Processing sensitive information

Sometimes it is necessary to process information about a person's criminal convictions, ethnicity, gender and family details. This may be to ensure NCIUL is a safe place for everyone, or to operate other NCIUL policies, such as the sick pay policy or equal opportunities policy. NCIUL will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes or disabilities. NCIUL will only use the information in the protection of the health and safety of the individual, but will need consent to process it, for example, in the event of a medical emergency.

Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for NCIUL to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason.

The Data Controller and the designated Data Protection Officer

NCIUL as a corporate body is the Data Controller under the Act, and NCIUL Executive Board is therefore ultimately responsible for implementation. However, the designated Data Controller for each department will deal with day to day matters relating to their department.

NCIUL has designated the Academic Quality Manager as the Data Protection Officer. Any query relating to the implementation within NCIUL of the GDPR 2018 and Data Protection Act 1998 should be referred to them. Subject Access Requests under section 7 of the Act will also be dealt with by the Academic Quality Manager.

All requests and any queries should be sent to:

Data Protection Officer
7 Skylines Village
Limeharbour
London E14 9TS

Examination marks

Students will be entitled to information about their marks for both coursework and examinations as part of their tutorial support. This is within the provisions of the Act relating to the release of data. However, this may take longer than other information to provide. NCIUL may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment borrowed from NCIUL have not been returned.

Retention of data

NCIUL will keep some forms of information for longer than others.

Data on students` health, ethnicity, disciplinary matters, fee payment, registration, careers support, disability support, study issues advice, course choice, use of student support services and day-to-day administration e.g. tutor allocation, graduation ceremonies, residential requirements, and enquiries will be destroyed 6 years after the student has completed their course or withdrawn from the module or programme.

Academic records which enable the institution to provide the Diploma Supplement and Transcript will be retained for the life of student i.e.120 years from date of birth. NCIUL will keep central personnel records indefinitely. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Please refer to the Records Retention Policy for further guidance on times of retention.

Guidelines for staff – Appendix 1

Members of staff will process personal data on a regular basis. NCIUL will ensure that staff and students give their consent to this and are notified of the categories of processing, as required by the Act.

Information about an individual's physical or mental health, religion and ethnicity is sensitive and can only be collected and processed with the individual`s express consent.
Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in NCIUL Data Protection Policy. In particular, staff must ensure that records are:

- allowed within the Act,
- accurate,
- up-to-date,
- kept and disposed of safely, and in accordance with NCIUL policy.

Individual members of staff are responsible for ensuring that all data they are holding is kept securely.

Members of staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the Data Controller in line with the NCIUL policy.

Staff checklist for recording data
Before collecting/processing any personal data, all staff should consider the checklist below.

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?

- Has the individual or data subject been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you notified Legal Services that you intend to hold the data?
- How long do you need to keep the data for, and what is the mechanism for review/destruction?

Glossary of terms

Data
Any information which will be processed or used on or by a computerised system or held as part of a filing system. This information can be written, taped or photographic.

Data Controller
A person who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

Data subject
The person about whom the data are held.

Personal data
Information about a living person. This information is protected by the Act.

Processing
Processing covers almost anything which is done with or to the data, including:

- obtaining data
- recording or entering data onto the files
- holding data, or keeping it on file without doing anything to it or with it
- organising, altering or adapting data in any way
- retrieving, consulting or otherwise using the data
- disclosing data either by giving it out, by sending it on email, or simply by making it available
- combining data with other information
- erasing or destroying data

Sensitive data
The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- their political opinions,
- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,
- their sexual life,

- the commission or alleged commission by them of any offence, or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

(NCIUL does not keep data in all of these categories – see Retention of Data)

Name of policy or procedure:	Data Protection Policy
Document owner:	Human Resources
Created:	03/2017
Last reviewed:	03/2019
Responsibility for review:	Human Resources Data Coordinator Equality and Diversity Committee
Date of next review:	010/2019
Related documents:	Data Privacy Statement Whistleblowing policy
Approved by:	HR Office April 2017
Equality impact Assessment undertaken:	04/2017
Version	
V2.4	Logo change