



**NEST ACADEMY**  
OF MANAGEMENT EDUCATION

# **DATA PROTECTION POLICY**

**Updated Version – January 2020**

## Table of Contents

1. Introduction .....	3
2. Scope .....	3
3. Aims.....	5
4. Data Protection Policy .....	6
5. Processing .....	6
6. Data Processing Officer.....	7
7. Responsibilities of Data User.....	7
8. Data Area and Data Area Contact.....	8
9. Data Areas.....	8
10.CCTV.....	12
11. Email.....	13
12.Sensitive Personal Data.....	13
13. Data Security Disclosure.....	14
14. Data subject Consent .....	14

## DATA PROTECTION POLICY

The information and guidelines within this policy are important and apply to the entire Institute community: The Owners, The Directors, Fellows Members and all staff and students (referred to collectively as the "Institute Community" in this policy). Non-compliance may result in disciplinary action

### INTRODUCTION

Like all educational establishments, the Institute holds and processes information about its employees, applicants, students, non-resident members and other individuals for various purposes (for example, the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll and to enable correspondence and communication, including the provision of references and certificates). The information must be collected and used fairly, stored safely and not disclosed to any unauthorized person. This document is designed to provide confidence in the College's confidential dealings with personal data in all areas of its operation.

### SCOPE

This policy covers records held and processed by Nest Academy of Management Education. It is responsible for its own records. For the purposes of this document, the following definitions will apply:-

#### **Personal Data:**

The Act applies to personal information that is subject to "processing". Information collected can be about living, identifiable individuals that is held either in a form in which it can be, or is being, processed automatically (this would, in the main, be on computer systems) or within a structured manual filing system. Statements of fact and expressions of opinion about an individual data subject are personal data as is an indication of the data controller's intentions towards the data subject. This

definition also includes data held visually in photographs or video clips (including Close Circuit Television footage) or as sound recordings. The Act also includes the processes using data, its use, retention, access, disclosure and final disposal.

### **Data Controller:**

Anyone who “processes data” is called a “data controller”. A data controller is a person (s) who determine(s) the purposes for, and the manner of, the processing of any personal data which and is required to comply with the eight principles of good information handling (the Data Protection Principles): These principles require the data controller to:

1. Process personal data fairly and lawfully.
2. Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner which is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
4. Ensure that personal data is accurate and, where necessary, kept up to date.
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Process personal data in accordance with the rights of the individuals to whom the information relates.
7. Ensure that personal data is kept secure, through use of appropriate technical and organisational measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

### **Data Subject:**

The individual who is the subject of the data entry

### **Data User:**

An authorised user of the personal data held by The College as data controller (for example, a member of staff or student).

### **Data application:**

How personal data held by The College is used within the context of the purpose for which it is held by the College

## **AIMS**

The lawful and correct treatment of personal information is vital to successful operations, and to maintaining confidence in the Institute Community and the individuals with whom it deals. Therefore, Nest Academy will, through appropriate management, and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;

- Ensure that the rights of people about whom information is held can be fully exercised. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information.)
- Take appropriate technical and organizational security measures to safeguard personal information;

## **DATA PROTECTION POLICY**

The Institute, as a Data Controller, must comply with the Data Protection Principles. In summary these state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes
- 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 those purposes.
- Be the subject of appropriate technical and organizational measures against unauthorized or unlawful processing, accidental loss or destruction.

Not be transferred outside Nest Academy.

## PROCESSING

"Processing", in relation to information or data, means obtaining, recording or holding the Information or data or carrying out any operation or set of operations on the information or Data, including:

- (a) Organization, adaptation or alteration of the information or data,
- (b) Retrieval, consultation or use of the information or data,
- (c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (d) Alignment, combination, blocking, erasure or destruction of the information or data.

## DATA PROCESSING OFFICER

Data Protection Officer is the Centre Head. All queries about the policy and all requests for access to personal data should be addressed to the Data Protection Officer (see "Right to Access Personal Data" below).

## RESPONSIBILITIES OF DATA USERS

All members of the Institute Community who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with the requirements of the Data Protection Principles and with the Institute's data protection policy (including any procedures and guidelines which may be issued from time to time). A breach of the Institute's data protection policy may result in disciplinary proceedings

In particular, no member of the Institute Community may, without the prior written authorization of the Data Protection Officer:

1. Develop a new computer system for processing personal data;
2. Use an existing computer system to process personal data for a new purpose;
3. Create a new manual filing system containing personal data;
4. Use an existing manual filing system containing personal data for a new purpose.

The above does not apply to databases which are maintained by individual Data Users within the Institute Community for their private domestic uses, for example, private address books. However, individual Data Users should consider whether their private domestic uses fall within the scope of this policy.

## **“DATA AREAS” AND “DATA AREA” CONTACT**

To aid the efficient administration of the data protection policy, the data which the Institute holds/processes has been divided into a number of "Data Areas": these are described below, showing who may have access to the data. In each case, there is also specified a "Data Area Contact".

He or she will be responsible in relation to the data in the Data Area in question (and thus not simply for the files which he or she maintains) for the following:

- Informing the Data Protection Officer of proposed processing of personal data within the Institute
- Providing personal data to the Data Protection Officer in response to a subject access request when requested to do so by the Data Protection Officer; and
- Maintaining the security of, and access to, personal data within the Data Area.

The Data Protection Officer may from time to time designate other Data Areas and/or Data Area Contacts. The Data Protection Officer or his appointee will have access to all of these data areas as required to achieve compliance with the Data Protection and Freedom of Information Acts.



## DATA AREAS

### Tutorial files

Tutorial files are maintained in respect of students' academic progress and welfare. They may also contain financial and medical data. The purposes for which they are maintained include monitoring students' academic progress and general welfare and administering the relevant student's applications for employment, professional training or admission to other educational establishments

Current Tutorial files are to be kept by the Academic Head. Tutorial files may be consulted on a day-to-day basis by the Academic Head, the students' own Tutor and Director of Studies and members of the secretarial staff in the Administrative Office. Tutorial files for past students are held in semi-current storage and may be consulted by the Academic Head and, with his/her permission, Fellows writing references. All other requests for access to a Tutorial file must be authorized by the Academic Head or the relevant Director of Studies.

*Data Area Contact: Academic Head*

### Student admissions files

Admissions files are maintained in respect of candidates, and potential candidates, for admissions. During the admissions process such files are maintained and kept by the Admission officer, the Graduate lecturers and their secretaries. For successful candidates, the admissions documentation is included in a Tutorial file. For unsuccessful candidates, the admissions documentation is retained for one year and then confidentially destroyed. During the admissions process, Admissions files may be consulted by the Academic Head, any of the Admission Officer, any Director of Studies and any other interviewers. All other requests for access to an Admissions file must be authorised by either of the Admissions Tutors or the Academic Tutor

*Data Area Contact: Academic Head*

### **Files relating to loans and grants made by the College to students**

These are maintained and kept by the Academic Head, their secretaries, and the Chief Accountant. These files may be consulted on a day-to-day basis by the Academic Head, the Graduate Tutors, their secretaries, the Chief Accountant, and senior staff in the Accounts Office. All other requests for access to any of these files must be authorised by the Academic Head for those held in the Administrative Office and the Chief Accountant for those held in the College Office.

*Data Area Contact:* Academic Head

### **Files in respect of any disciplinary matters involving students**

All such files are to be maintained and kept by the Academic Head or his/her secretary, who may each consult the same on a day-to-day basis. Sensitive information is placed in a sealed envelope in the student's Tutorial File. All other requests for access must be authorised by the Academic Head.

*Data Area Contact:* Academic Head

### **Medical files in respect to Student health and welfare**

Medical files are to be maintained and kept by the College Nurse, who may consult the same on a day-to-day basis. All other requests for access to medical files must be authorised by the College Nurse.

*Data Area Contact:* College Nurse

### **Medical notes in respect of students**

Such notes are maintained by the Senior Tutor in the student's Tutorial file for health and safety reasons, to assist in meeting the needs of students with disabilities, or for reasons connected with absences from College, poor performance, applications to the University or to charities etc.

All current notes in this category are to be kept by the Academic Head. Sensitive information is placed in a sealed envelope in the student's Tutorial File. The notes may be consulted on a day-to-day basis by the Academic Head, the students' own Tutor and the

Academic Head's Assistant. All other requests for access to these notes must be authorised by the Academic Head

*Data Area Contact:* Academic Head

### **Personnel files in respect of other employed staff of the College**

These are maintained and kept by the Personnel Manager. These files may be consulted on a day-to-day basis by the Personnel Manager, the Chief Accountant, senior Accounts Office staff, any Head of Department (for their own staff only), and their secretaries. All other requests for access to these files must be authorised by the Personnel Manager.

*Data Area Contact:* Personnel Manager

### **Wages files in respect of employed staff and Fellows**

These are maintained and kept by the Chief Accountant and Accounts Office staff. These files may be consulted on a day-to-day basis by the Chief Accountant and Accounts Office staff. All other requests for access to these files must be authorised by the Chief Accountant.

*Data Area Contact:* Chief Accountant

### **Files relating to tenancies of College properties, suppliers of goods and services to the College, and other third parties not otherwise dealt with in this policy document**

These are maintained and kept by the Admin Office, their respective staff, the Chief Accountant, and the Accommodation Officer. These files may be consulted on a day-to-day basis by the Admin Manager, the Accommodation Officer, the Chief Accountant, and Accounts Office staff. All other requests for access must be authorised by them.

*Data Area Contact:* Admin Manager

### **College Archives**

The individual files relating to members of the College Community are the basis of the non-resident member records and detailed historical archives of the College, and may be retained indefinitely for reference and research purposes.

At some point after a member of the College Community leaves the College, his or her file(s) will be transferred to the Semi-Current Record Store, then to the Archive Centre. The timing for this will differ from Data Area to Data Area, and within each Data Area will depend upon a number of factors.

The College reserves the right to destroy (in whole or in part) archived files whenever it considers it appropriate to do so.

*Data Area Contact: Admin Manager*

### **Computer Databases**

Certain of the files referred to above are maintained in electronic databases as well as, or instead of, paper files. Access to such databases is restricted in the same manner as access to paper files in the relevant Data Area.

In addition, however, the IT Manager and Computer Officer may have day-to-day access to the electronic databases for the purposes of administering and maintaining the same.

*Data Area Contact: IT Officer*

## **CCTV**

The College operates a number of CCTV cameras in order to assist with security for members of the College Community and in respect of College property. If you have any queries regarding the operation of the CCTV system, please speak to the Admin Officer, The tapes are held in secure conditions. If you wish to access any personal data about you on the CCTV system, you are asked to complete and return an Access to Personal Data form

## EMAIL

It is permissible and appropriate for the Institute to keep records of internal communications which are relevant to an individual's ongoing relationship with the , whether as a Fellow, member of staff or student, including information concerning performance and conduct issues, provided such records comply with the Data Protection principles.

It is recognized that email is used for such communications and that such emails should form part of the Institute's records. It goes beyond the scope of this policy document to address the appropriate use of email in the proper functioning of the Institute, and the limitations and legal implications with this mode of communication. However, all members of the Institute Community need to be aware that:

- Emails which contain personal data about individuals which are sent or received by members of the Institute Community (other than for their own private purposes as opposed to Institute's purposes);
- Subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the institute to locate the personal data in the emails; and
- The legislation applies to all emails from and to members of the College Community which are sent and received for College purposes, whether or not the emails are sent through the College email system or on an individual's own email account

## SENSITIVE PERSONAL DATA

The College may from time to time process "sensitive personal data" relating to admissions candidates, members and staff of the In

"Sensitive personal data" is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject,

The Institute envisages the need to process sensitive personal data of a type specified in the consent forms set out in Schedule to this policy for the purposes specified. For example, data relating to the ethnic origin of members or staff of the Institute may be processed for the purposes of equal opportunities monitoring or to identify any necessary dietary requirements and possible

sources of financial assistance. Medical records need to be processed for the provision of healthcare and general welfare, to identify any necessary dietary and accommodation requirements and to assist in meeting the needs of members of the Institute's with disabilities. In exceptional circumstances, the Institute may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

## DATA SECURITY DISCLOSURE

All members of the Institute's Community are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.
- Unauthorized disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the Institute Data Protection Officer.
- Personal data must be kept securely and examples of how this may be done will include:
  - ✓ Keeping the data locked in a filing cabinet, drawer or room; or
  - ✓ If the data is computerized, ensuring that the data is password protected or kept only on disk which is itself kept securely; orAny other appropriate security measure needs to be taken

## DATA SUBJECT CONSENT

Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. However, it is the Institute's policy to seek express consent whenever practicable from individual data subjects for the main ways in which the Institute may hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The College will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law.

Therefore, all prospective Fellows, staff, admissions candidates and students will be asked to sign a consent form regarding particular types of information which the Institute may in due course

hold/process about them. Existing Fellows, staff and students will also be asked to sign a consent form

### **Nest Academy Data Protection: Request for Access**

Please provide the following details, which will help us to process your request. The completed form should be sent to:

Centre Head,

Nest Academy of Management Education

SURNAME	
FIRST NAME	
ADDRESS	
DAY TIME TEL NUM	
EMAIL ADDRESS	

ARE YOU A STUDENT OR A FORMER STUDENT?	YES/NO
WHAT DID YOU STUDY AT NEST ACADEMY?	
YEAR OF REGISTRATION	
YEAR OF LEAVING / COMPLETION	

ARE YOU A MEMBER OF STAFF OR A FORMER MEMBER OF STAFF	YES/NO
WHAT DEPARTMENT(S) DID YOU WORK IN?	
YEARS EMPLOYED AT COLLEGE	
ANY INFORMATION THAT MAY HELP US	

Entry under which you would like a copy of the information held about you by the Institute

CATEGORIES	PLEASE TICK
Academic Department: Administrative records (excluding Assessments and Exam information)	
Academic Department: Assessment and Exam information	
Flexible Learning Centre / Learning Centre	
Administrative Department: Estates	
Administrative Department: Exams	
Administrative Department: Finance	
Administrative Department: Human Resources	
Administrative Departments: IT Services	
Administrative Department: Marketing	
Administrative Department: Management Information Services (excluding Exams)	
Administrative Department: Student Services	

SIGNATURE: .....

Date:.....

NAME .....



**OFFICE USE ONLY**

Date Request received

.....

Request received by

.....

Information Provided

.....  
.....  
.....  
.....

Signed

Job Title