Nescot
Epsom's college of further and higher education

Data Protection Policy

Author/Reviewer:	Assistant Principal IS
Date Approved:	Feb 2004
Where Approved:	Corporation
Date of Issue:	Nov 2008
Impact Assessment:	Nov 2010

Written	Review date	Review date	Review date	Review date
Feb 2004	Nov 2008	Nov 2010	July 2012	

Data Protection Policy

Introduction

Nescot needs to keep certain information about its employees, students and other users to allow it to monitor, for example, performance, achievements, and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government fulfilled. To comply with the law, information must be collected and used fairly, stored safety and not disclosed to any other person unlawfully. To do this, Nescot must comply with the Data Protection Principles (see Appendix 1) which are set out in the 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.

All College staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Nescot has adopted this Data Protection Policy.

The Data Protection Officer is Dario Stevens, Assistant Principal Information & Planning.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Nescot.. Any failures to follow the policy can therefore result in disciplinary proceedings.

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated Data Protection Officer. If the matter is not resolved it should be raised as a formal grievance or complaint. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

Notification of Data Held and Processed

All staff, students and other users are entitled to:

- know what information the College holds and processes about them and why;
- know how to gain access to it;
- know how to keep it up to date;
- know what the College is doing to comply with its obligations under the 1998 Act.

The College has made a standard form of notification available to all staff, students and other relevant users. This states all the types of data the College holds and processes about them, and the reasons for which it is processed. This is contained in the in Appendix 3 to this document.

Responsibilities of Staff

All staff are responsible for:

- checking that any information that they provide to the College in connection with their employment is accurate and up to date;
- informing the College of any changes to information, which they have provided, e.g. changes of address;
- checking the information that the College will send out from time to time, giving details of information kept and processed about staff;
- informing the College of any errors or changes to information that they are responsible for. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines provided to them.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is 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.

- Personal information in the form of manual records should be:

- kept in a locked filing cabinet; or
- locked drawer; or
- other secure area

- Personal information in the form of computerised records should be:

  - password protected on the college network/intranet; or
  - in an area of the college network/intranet where access is limited; or
  - kept only on a data storage device (such as CD-ROM or portable data stick which itself encrypted and secure

Student Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address, etc are notified to Advice & Guidance.

Students who use the College computer facilities may, from time to time, process personal data. If they do, they must notify the Data Protection Officer. Any student who requires further clarification about this should contact the Data Protection Officer. (see also Student IT Use Agreement).

Rights to Access Information

Staff, students and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain paper files.

Any individual who wishes to exercise this right should do so in writing preferably using the standard form available in appendix 2 of this document. Requests should be sent to the Data Protection Officer.

The College reserves the right to make a charge of £10 on each occasion that access is requested in addition to the direct costs of producing the information.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is the College policy to make as much information public as possible. The Freedom of Information Act 2000 also gives you the right to ask any public body for all the information they have on any subject you choose unless an exemption in the Act legitimately applies. Requests must be made in writing and the College has 20 working days in which to respond. In order to comply with this act the College has a Freedom of Information Publication Scheme available its website.

However, in addition to this certain personal data will be available to the public for inspection:

- Names of college governors;

- Register of interests of Governing Body members and senior staff with significant financial responsibilities

- Lists of key staff

The College internal phone list will not be a public document.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Protection Officer.

Subject Consent

In many cases, the College 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 the College 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.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 1 6 and 18. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The College also has a duty of care to all staff and students and must therefore make sure that employees and those who use the College facilities do not pose a threat or danger to other users.

The College 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. Nescot will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies, such as the sick pay policy or equal opportunities policy. It is also necessary to meet the College's obligations to disabled staff and students under the provisions of the Disability Discrimination Act. 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 the College to do this. Therefore, all prospective staff will be asked to give their consent to processing sensitive data on the appropriate forms: Application Form, Consent to Process Medical Information Form and Equal Opportunities Monitoring Form. Students will be asked to for consent to process information on the enrolment form and to sign a "Sharing Information Agreement" when there is a need to process sensitive information. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information is available from Human Resources (staff) or the Advice & Guidance Centre (students).

Telecommunications, CCTV and IT infrastructure

Computer accounts are the property of the college and are designed to assist in the performance of the work of employees and students. There should, therefore be no expectation of privacy in any stored work or messages sent or received, whether of a business or of a personal nature.

When sending e-mails on the College's system, the sender is consenting to the processing of any personal data contained in that e-mail and is explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If individuals do not wish the College to process such data they should communicate it by other means.

The college has the right to monitor any and all aspects of its telephone and computer systems, and to monitor, intercept and/or record any communications made or received by employees, including telephones, email or Internet communications.

Employees and students should be aware that Close Circuit Television (CCTV) is in operation for their protection and the security of college property.

Further information is available in the College's Acceptable IT Usage Agreements.

The Data Controller and the Designated Data Controllers

The College as a body corporate is the data controller under the Act, and the Corporation is therefore ultimately responsible for implementation. However, designated data controllers will deal with day to day matters.

The role of the Data Controller is to:

- to ensure that all data is processed fairly;
- to ensure that the data is accurate, and that processes exist to check and amend data as necessary;
- to ensure that consent is obtained either generally or expressly;
- to ensure that policies and procedures are in place to enable access by those whom the data concerns;
- to ensure that data is kept securely and disposed of properly;
- to make sure the notification requirements are satisfied;
- to make determinations regarding processing of data without consent, in cases of necessity or public interest.

The College designated data controllers are:

Dario Stevens	Data Protection Officer Assistant Principal Information & Planning
Barry Wastnidge	Assistant Principal Corporate Services & HR
Carol Martin	Deputy Principal
Rob Greening	Director of Faculty
Janice Davies	Director of Skills & Learning Support
Lindsey Biggs	Director of Employer Engagement
Iain Gibbins	Director of Information Learning Technology
Jacqui Udy	Director of Student Services & Marketing

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all College books and equipment have not been returned to the College.

Retention of Data

The College will keep some forms of information for longer than others. Because of storage restrictions, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept for a minimum of six years after they leave the College.

Nescot will also need to keep information about staff. In general, all information will be kept for six years after a member of staff leaves Nescot. Some information however will be kept for much longer. 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. A full list of information with retention times is available from the designated data controllers.

A list of the archiving retention times employed by the College is included as appendix 4.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of Nescot. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer.

Associated Documents and Policies

- Staff Guideline for Data Protection
- Freedom of Information Publication Scheme
- Data Access Policy to Staff and Student IT Accounts
- ICT Security Policy
- Staff Acceptable IT Usage Agreement
- Student Use IT Agreement

Appendices

1. The Eight Data Protection Principles
2. Subject Access Request Form
3. Notification of Personal Data
4. Guidelines for Retention of Personal Data

Appendix 1 to Data Protection Policy

The Eight Data Protection Principles

1. Personal Data must be processed fairly and lawfully and shall not be processed unless certain conditions are met.

2. Data must be obtained only for specified and lawful purposes and must not be processed in any way that is incompatible with that purpose.

3. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

4. Personal Data shall be accurate and kept up-to-date.

5. Personal Data processed for any purposes shall not be kept for longer than is necessary for those purposes.

6. Personal data shall be processed in accordance with the rights of the data subjects under this Act [Data Protection Act 1998].

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix 2 to Data Protection Policy

Subject Access Request Form (Data Protection Act 1998)

The Data Protection Act 1998 gives students, staff and other users of the College the right to access personal data relating to themselves that is held by the College as part of a 'relevant filing system' (both in electronic and paper format). Any individual who wishes to access data should apply using this form.

The College needs to be assured of the applicant's identity before relevant data is released and a fee (£10.00) is due when a request for the release of data is made. Please note that the College may require a maximum of 40 days in which to supply the requested information.

1) ARE YOU THE DATA SUBJECT?

Yes – are you applying for data the College holds about you? You will need to supply the College with evidence of your identity (student/staff ID card, proof of address, driving licence, birth certificate (or photocopy) etc.) as well as a signed copy
of this form. This is to ensure we only release data to those who have a right to see
the information.

Now complete items 2, 4 and 5 below

No - are you acting on behalf of the Data Subject with their written authority? If so, you will need to enclose an original copy of their permission to disclose. This can be a letter which is signed personally by them giving you authority. We must be able to confirm from our records that this request relates to the Data Subject. You will be the applicant. The Data Subject details must be included in item 3 below.

Now complete items 2, 3, 4 and 5 below

2) DETAILS OF APPLICANT

Full Name ……...

Address (including postcode): …….

Telephone number (day): ……Mobile: ……...

Email Address: …….....

3a) DETAILS OF THE DATA SUBJECT (if different to 2)

Full Name ……...

Address (including postcode): …….

Telephone number (day): ……Mobile: ……...

Email Address: …….....

3b) Why are you making the request on behalf of the Data Subject?

…….....

…….....

…….....

…….....

4a) STUDENTS

Are you a current or past student of this College? **Current / Past / Not a student**

If you are a current student, please provide your course title :

…….....

For past students, please provide your course title and dates of study:

…….....

4b) STAFF

Are you a current or past member of staff? **Current / Past / Not a staff member**

If yes, please provide us with the name of your department:

…….....

For past staff, please give dates of employment and position held:

…….....

4c) OTHERS (neither student nor staff)

If neither a student nor a staff member please provide details of your connection with the College:

…….....

…….....

5) INFORMATION REQUIRED

The College may hold personal records in different parts of its organisation. Please be specific if there is particular information that you require and if possible identify where you think this information will be held:

…….....

…….....

…….....

…….....

…….....

Signed:……

Date:……..

Please return the form to Data Protection Officer, North East Surrey College of Technology, Reigate Road, Ewell, Surrey KT17 3DS.

Documents which must accompany this application are:

i evidence of your identity
ii evidence of the Data Subject's identity (if different from above)
iii evidence of Data Subject's consent to disclose to a third party (if required asindicated above)
iv a fee of £10 (cheques to be made payable to NESCOT)
v stamped addressed envelope for return of proof of identity/authority documents,where appropriate

Please note that the College reserves the right to obscure or suppress information that relates to other third parties (under the terms of Section 7 of the Data Protection Act 1998)

Appendix 3 to Data Protection Policy

Notification of Personal Data held by the College

This notice sets out the types of personal data that this College currently holds about you, and gives details of that data.

We currently hold information in the following categories:

Students:

- Personal details: this includes, name, date of birth, ethnicity, gender, address, contact numbers, email address, prior qualifications, previous school, next of kin
- Where disclosed details of physical and/or mental health: this could include details about specific conditions individuals may suffer from, such as asthma or diabetes and information
- about pregnancy (if appropriate)
- Details about student academic performance and expected results, references and recommendations and attendance.
- Details about student course fees, course registration, library and other equipment on loan.
- Details about any criminal record self-disclosed

Staff:

- Personal details: this includes, name, ethnicity, date of birth, address, contact numbers, email address, qualifications, gender, religion/belief, sexual orientation, marital status
- Where disclosed details of physical and/or mental health: this includes details about specific conditions individuals may suffer from, such as asthma or diabetes: information about pregnancy, if appropriate, information about sickness absences
- Details about employees work performance, including notes of supervision sessions, appraisals, and training assessment.
- Personnel information. This includes details about start date; pension and pay details; your next of kin; any current disciplinary or grievance matters; any deductions from salary or any loans.
- References from previous employers

Appendix 4 to Data Protection Policy

Guidelines for Retention of Personal Data

(This is not an exhaustive list. Medical records are kept for a variety of health and safety reasons, and will carry their own retention times.)

Type of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 1 year from the date of the interviews.	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records relate	Statutory Sick pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHHR 1994
Student records, including academic achievements, and conduct.	At least 6 years from the date the student leaves Nescot in case of litigation for negligence. At least 10 years for personal and academic references, with the agreement of the student. At least 10 years for those records where funding from the European Social Fund (ESF) has been received by the College or the Skills Funding Agency (SFA).	Limitation period for negligence