



New College Durham

Policy on Data Protection

DOCUMENT HISTORY

Issue No.	Consultation Detail	Date of Consultation	Approved by	Date Approved	Details of Amendment/Review
1	ICT Dept Director of Finance and Corporate Services	December 2005 – March 2006	Corporation	20.03.06	
1.2	SEG	December 2006	SEG	14.12.06	Addition of two new guidelines.
2	SEG	January – March 2007	Corporation	14.03.07	Annual review.
3	ICT Dept SEG	January-March 2008	Strategy & Resources Committee	06.02.08	Addition to policy statement. Format for data sharing agreements. Reference to the use of personal data on website.
3.1	ICT Dept	December 2012	Department	11.12.12	Amendment of review date.
4	ICT Information Compliance Group	March 2013	Strategy & Resources Committee	27.06.13	Full Review. Minor amendments. Reference to Privacy Impact Assessments

Data Protection

1. Introduction

The Data Protection Act 1998 (DPA) gives rights to individuals, including employees, about whom information or “personal data” is obtained or processed, whether manually or electronically. The College is committed to fulfilling its obligations under data protection legislation in respect of all processing of personal data in connection with its business and in so doing meeting the expectations of its employees, customers and suppliers.

2. Scope of the Policy

a. What is Personal Data?

Personal data is information that can be used to identify a living individual (sometimes called the ‘data subject’). Examples of personal data which may be used by the College include addresses, telephone numbers, CVs, photographs, CCTV footage and statements of opinion or intention regarding individuals.

Some information is considered to be “Sensitive Personal Data”. This includes information relating to:-

- i. race or ethnic origin;
- ii. political opinions;
- iii. religious or similar beliefs;
- iv. trade union membership;
- v. physical or mental health or conditions;
- vi. sexual orientation/behaviour; or
- vii. information relating to the commission or alleged commission of any offence and any related court proceedings.

There are special rules to follow when processing Sensitive Personal Data.

b. What is Processing?

The College will be processing personal data if it holds personal data and/or carries out any operation relating to that information such as altering or deleting it, accessing, downloading, reviewing or transferring it. It is irrelevant whether the information is stored as a manual or electronic record.

3. Responsibilities

The College has responsibility to collect and hold information in accordance with the DPA. Ultimate responsibility for ensuring compliance with this policy lies with the Corporation.

The College Information and Records Manager has day-to-day responsibilities for co-ordinating the College Data Protection function. These responsibilities include ensuring associated Data Protection guidelines are available and promoting compliance with the provisions of these guidelines.

All staff have responsibilities under the DPA and are responsible for:-

- a. familiarising themselves with this policy and any relevant Data Protection guidelines;
- b. dealing with all requests within 40 working days of receipt;
- c. contacting the Information and Records Manager when assistance is required.

Compliance with this Policy is compulsory for all staff employed by the College. A member of staff who fails to comply with the Policy may be subjected to disciplinary action under the College disciplinary policy. It is the responsibility of Heads of Departments/School and their Directors to ensure that their staff are made aware of the existence of this policy and its content.

Employees should be aware that they may also face criminal liability in certain circumstances.

4. Relationship with Existing Policies

This Policy has been formulated within the context of the following College documents:-

Freedom of Information Policy
Records Management Policy
Information Security Policy
Electronic Communications Internet and Telephone Monitoring Policy

5. Guidance for Processing Personal Data

a. Notification

The College is required to notify the Information Commissioner about the processing of any personal data. The College has notified its processing accordingly and is only permitted to process data within the remit of its Notification. Notifications are reviewed on an annual basis by the Information and Records Manager. Detail of the College's Notification can be accessed via the ICO [website](#).

If any department creates a manual or electronic system or record which contains personal data, the Information and Records Manager should be informed to ensure that the College entry on the Data Protection Public Register is up-to-date.

b. Use of Personal Data Must be Fair and Lawful

The College must ensure that wherever possible individuals are advised of the personal data which has been obtained or retained, its source and the purposes for which the personal data may be used or disclosed. Where applicable consent must be obtained to use the information.

If the details about the intended processing are known to the individual at the time the personal information is collected then consent will be deemed given. If the information is not received directly from the individual then the College must ensure that it has authority to use this information. However, the College must have the explicit consent of the individual to process Sensitive Personal Data and in this circumstance consent cannot be deemed. If there is no explicit consent or the information has not been received directly from the individual, the College will not process this information unless it obtains the relevant consents or is otherwise lawfully entitled or obliged to do so.

If the reasons for processing data change, then the data subject must be notified.

Occasionally there may be a justification to process without consent. However, only the Senior Information Risk Owner may authorise this.

c. Use of Personal Data Must be Justified

The personal data processed by the College must be adequate, relevant and not excessive for the College's purposes. Methods of data capture must:-

- i. be specific to the particular processing purpose;
- ii. obtain all personal information necessary on which to base any decision that is to be taken for the processing purpose;
- iii. not collect personal data that is not necessary for the processing purpose for which the individual has provided details, or which is to be used for another purpose (ie marketing) about which the individual has not been informed;
- iv. ensure that the data subject is informed at the time the information was collected of the processing purpose.

d. Personal Data Must be Accurate

The College will take all reasonable steps to ensure that personal data held in its systems is accurate.

e. Personal Data Must be Held No Longer Than Necessary

The College must not keep information for longer than is necessary for the purpose for which it is being processed. The retention of personal data is covered by the College's Records Retention Schedule. Information about retention requirements can be obtained from the College Information and Records Manager.

f. Personal Data Must be Processed in Accordance with Individuals' Rights

Individuals have the right to:-

- i. have information made available on request;

- ii. request that the College does not process information which will or is likely to cause substantial and unwarranted damage or distress to them;
- iii. be notified of any decisions made solely on the basis of automatic processing, such as performance at work, reliability or conduct and the logic for that decision making;
- iv. have any decision based solely on automatic processing to be reviewed upon written request; and
- v. prevent the College from taking any decision which significantly affects the individual based solely on personal information processed by automatic means.

g. Appropriate Security must be Applied to all Personal Data

The College must have appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing, accidental loss of or destruction or damage to personal information.

Any third party processing personal information on behalf of the College must sign a declaration of confidentiality and undertake to process the information under this Policy.

In addition, any arrangement to share personal data with any third party must be documented using the Data Sharing Agreement Form which details what types of data are shared and what procedures are in place to ensure the security of the data.

i. Transfers outside the European Economic Area

All transfers of personal information outside the European Economic Area must be approved first by the Information and Records Manager. This includes the use of personal data on the College website.

ii. Direct Marketing

The College must not directly market to any individual without obtaining prior consent to do so. The College will comply with any request by an individual not to receive direct marketing information.

iii. Access to Information

All requests must be dealt with within 40 days of receipt of the request from the individual in writing, together with a £10.00 access fee made payable to New College Durham. The Information and Records Manager should be notified of any non-routine requests received. Non-routine requests are requests for information that the member of staff concerned would not normally provide as part of their job.

iv. Privacy Impact Assessments

Where appropriate a privacy impact assessment will be carried out by the Information and Records Manager. The assessment will be reported to the

Information Management Steering Group as part of the project approval process.

Further Guidance:-

Guidance Note 1: Making a Data Protection Request

Guidance Note 2: Data Protection for Staff

Guidance Note 3: Data Protection for Students¹

Guidance Note 4: Best Practice Advice for Data Protection

Guidance Note 5: Disclosure of Information to the Police

Guidance Note 6: Disclosure of Information on Staff and Students

Guidance Note 7: Protecting and disclosing student information

Guidance on the Disposal of Confidential Waste

Guidance on Providing References

6. Contact Details

To make enquiries about the College's Data Protection Policy please contact the Information and Records Manager at records@newdur.ac.uk or on (0191) 375 4422.

7. Evaluation and Review

The performance of this Policy will be reported on annually and it will be formally reviewed every five years by the Corporation.

In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

Last Review: March 2013

Review Due: March 2018

¹ A copy of this guidance is made available to students at enrolment