Data Protection Policy 2013 - 2016

Issue 3

March 2013

Summary of Policy:

This policy sets out the approach taken by the College to comply with its legal and regulatory obligations under the Data Protection Act (1998).

Senior Manager Responsible for Policy:

Susan Ross
Director of Funding & Planning

1.0 STATEMENT OF POLICY AND COMMITMENT

This Policy Statement summarises the approach taken by the College to comply with its legal and regulatory obligations under the Data Protection Act (1998), and to contribute to the effective overall management of the institution. The College will seek to meet its obligations in law, and in spirit, with regard to the appropriate handling of data.

The College supports the rights of individuals to gain access to personal information held about them by the College and the right to challenge the accuracy of data held.

It is College policy for all data processors and users within the College, whether students, staff or others, to comply with the law and for the College to provide guidance to enable them to achieve this. For the purpose of this policy, data is information held in any form, including written notes, records, and electronic. College data should be collected, used fairly, stored safely, disposed of correctly and may be disclosed only within constraints laid down in law. The College will identify data typically used within the College, and identify who within the College may be contacted to obtain further guidance or clarification. In particular the College will:

- observe the 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 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 under the Act. (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 organisational security measures to safeguard personal information
- ensure that personal information is not transferred abroad without suitable safeguards

Clear guidelines in the form of a document entitled “Data Protection Policy – Supplementary Procedures and Guidelines” have been placed on the College’s VLE, Moodle. They expand on the following topics:

- Responsibilities of individual data users
- Procurement, storage, disposal and release of personal data
- Teaching and assessment procedures
- Supplying, requesting and receiving 'confidential' references

- Applications and interviews
- Photographs, videos and closed circuit television
- Marketing Information
- Medical data
- Processing sensitive Information

1.1 Notification to the Data Protection Commissioner

The College, as a Data Controller, will notify the Information Commissioner of the purposes for which it processes personal data. Individuals can obtain full details of the College's data protection register entry with the Information Commissioner from the College's Director of Funding and Planning or from the Information Commissioner's website (http://www.dataprotection.gov.uk)/

1.2 Personal Data

1.2.1 Information Entitlement

All staff, students, and other users are entitled to:

- Know what personal information Tyne Metropolitan College holds and processes about them and why, and that they have the right to access personal information.
- Know how to gain access to personal information by following correct procedures.
- Give and receive feedback on inaccuracies in data disclosed in this way so correction can be carried out.
- Know how to keep personal information up to date.
- Know what Tyne Metropolitan College is doing to comply with its obligations under the 1998 Act.
- A response from the College for requests for access to personal data, normally within 40 working days of the request, or payment of the administration fee, whichever is the later.

1.2.2 Definition of Data

In the terms of the Act, is information relating to an individual where the structure of the data allows information about the individual to be readily accessed. The information may be held in manual form (e.g., as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically.

- Personal data is any data relating to a living individual (e.g., name, address, payroll details, and exam results).
- Sensitive data from a subset of personal data that relate to a living person, recording such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, criminal convictions, etc. (Special considerations apply if sensitive data is to be

processed, and advice must be sought from the Head of Service: Network & IT prior to processing.)

- Data is processed whenever compiled, stored or otherwise operated upon. Thus actions such as disseminating the examination results of students involves processing data relating to each of them, as does giving and receiving personal references, producing agenda items or minutes for committees at which students are discussed as individuals, etc. Similarly, data about staff are processed when they are committed to manual or electronic records held within the institution.

1.2.3 Data Protection Principles

The Act requires that all staff, students and others who process or use any personal information at the College must ensure that they adhere to Eight Data Protection Principles. Disciplinary action may be taken against any staff member or student who breaches any of the instructions or procedures following from this Policy. In summary these require that personal data shall be:

I. obtained and processed fairly and lawfully and shall be processed according to the requirements of the Act

II. obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose

III. adequate, relevant and not excessive for those purposes

IV. accurate and kept up-to-date

V. kept for no longer than is necessary

VI. processed in accordance with the data subject's rights

VII. be kept safe from unauthorised access, accidental loss or destruction

VIII. transferred, where requested, to a country only within the European Economic Area (the EU member states, plus Norway, Iceland and Liechtenstein), unless such a country has equivalent levels of protection for personal data.

All staff and others who process or use any personal information must ensure that they follow these principles at all times. For further advice please see the "Data Protection Policy – Supplementary Procedures and Guidelines" (located on the College's VLE, Moodle.)

2.0 RESPONSIBILITIES FOR IMPLEMENTING THE POLICY

The College Senior Manager with overall responsibility for this policy is the Director of Funding and Planning.

2.1 Governors are responsible for ensuring that:

- They understand Data Protection Act (1998), and the College's obligations to process data fairly, transparently and for specific purposes under the Act.

- They seek to meet these obligations.

- They support an ethos within the College to promote transparency and openness in relation to the information it holds

2.2 The Head of Service: Network & IT is responsible for:

- Maintaining guidance information for processing and handing requests under the Act.
- Encouraging the practice and promoting compliance with this policy.
- Supporting Department Managers to help them comply.
- Provide training when appropriate.

2.3 Managers are responsible for ensuring that:

- Their staff are made aware of the existence and content of the Policy and the Act.
- They and their staff understand the requirements of the Data Protection Act (1998)
- Practices and systems within their area of responsibility follow the College Policy, Procedures & Guidelines, and those data held within their area are accessible as prescribed by both the Freedom of Information Act and the Data Protection Act.
- Staff use the appropriate permission forms shown in the "Data Protection Policy – Supplementary Procedures and Guidelines" when formally seeking permission to process extraordinary data.
- The Human Resources department must ensure that sufficient and up to date training is given to all managers and staff

2.4 Staff are responsible for ensuring that:

- They meet their responsibilities under the Act, whether or not they create, receive or maintain information.
- Information they process is handled in compliance with this Policy, and associated Procedures & Guidelines. In general, staff are responsible for:
    - Familiarising themselves with the Data Protection Act (1998), this Policy, and College Guidelines
    - Providing advice and assistance to persons making requests for information
    - Dealing with all requests within 40 days of receipt
    - Contacting the Head of Service: Network & IT when assistance is required
    - Using the appropriate permission forms shown in College Procedures & Guidelines, when formally seeking permission to process extraordinary data.

2.5 Learners are responsible for ensuring that:

- They support the College in its implementation of the policy whenever it is appropriate to do so.

3.0 LEGAL DUTIES

- Data Protection Act (1998)
- Freedom of Information Act (2000)
- Other legislation and legislative updates as appropriate.

4.0 GUIDELINES FOR IMPLEMENTING THE POLICY

4.1 **The public** (including learners, work placement providers and staff)

- The College's Data Protection Policy and associated guidelines will be published on the College's website.

4.2 Staff

- The latest version of the policy and associated guidelines will be located on the services area of the College's VLE, accessible to all College members.
- Procedures and guidelines for implementing this policy are available in a separate document entitled "Data Protection Policy – Supplementary Procedures and Guidelines", available on the College VLE.
- Further information & guidance documents are available:
    - "The Data Protection Act at Tyne Metropolitan College" available on the VLE, Moodle and in the appendix of document "Data Protection Policy – Supplementary Procedures and Guidelines".
- The College has arranged mandatory training sessions on the Data Protection Act for all staff, at which College policy and guidelines are referenced.
- Human Resources Management are responsible for, and will ensure, the induction of new staff, permanent and temporary, into the existence and use of all policies.
- Any questions or concerns about the interpretation or operation of this policy should be taken up with the Head of Service: Network & IT.

4.3 Learners

- The Director of Learner Services should ensure all relevant policies are referenced during learner induction to the College.
- Any questions or concerns about the interpretation or operation of this policy should be taken up with the Head of Service: Network & IT.

4.4 Monitoring and Positive Action for Implementing the Policy

- It is the responsibility of all managers to ensure the policy is implemented in the College.

- The Head of Service: Network & IT will periodically send reminders to staff on their responsibilities under the act, to ensure the act remains in the forefront of people's minds.
- Formal Data Protection Requests that are not easily processed by staff are channelled via the Head of Service: Network & IT, who maintains a record of such requests or any complaints that have passed through his office. These stimulate a review and update of procedures and guidelines where deemed appropriate.

5.0 CONTROL OF THIS DOCUMENT

This document was prepared by, and is issued, controlled and modified by the Head of Service: Network & IT after due authorisation from the Corporation Board. It will be reviewed every three years or earlier if circumstances warrant it.

The latest version of the document will be maintained on the College's website and internal VLE (Toolkit).

Please feed back to the Head of Service: Network & IT any constructive suggestions on how any aspect of the document may be clarified or improved upon.

Prepared by:	**Director of Funding & Planning**
Equality Impact Assessed by:	**Head of Service: Network & IT**
Validation & tracking by:	**Executive Officer**
Corporation Approval:	**D.W. Midgley** **Signed:……** **26 March 2013** **Date:……**
To be reviewed:	**March 2016** **Date:……**