THE NORTHERN COLLEGE

DATA PROTECTION POLICY

Denise Pozorski
Vice Principal (Residential & Administrative Services)
Revised March 2015

Introduction

The Northern College needs to keep information about its students, employees and other users. It is necessary to process this information so that courses can be organised, staff recruited and paid, and statutory obligations to funding bodies and other organisations complied with. To remain within the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Northern College must comply with the Data Principles 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 in relation to the purpose for which they are held
- be accurate and kept up to date
- be kept no longer than is necessary for the purpose for which they are held
- 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 staff, governors, students or others who process or use any personal information must ensure that they follow the above principles at all times. It is intended that this Data Protection Policy will help to ensure that this happens.

Personal data is defined as information about a living person that by itself, or in conjunction with other information which is kept in a manual or computerised system, is sufficient to identify an individual. This information is protected by The Act.

"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, including the outcome of those proceedings.

The college will have records of internal communications which are relevant to an individual's ongoing relationship with the college, whether as a, member of staff or student, including information concerning performance and conduct issues, and such records should comply with the Data Protection principles.

It is recognised that email is used for such communications and that such emails should form part of the college's records. All members of the college community need to be aware that:

- the 1998 Act applies to emails which contain personal data about individuals which are sent or received by members of the college community (other than for their own private purposes as opposed to college 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 college 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.

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 adopted by the Northern College from time to time. Any failure to follow the policy may therefore result in disciplinary proceedings.

Any member of staff or student who considers that the policy has not been followed in respect of their own personal data should raise the matter with the Vice Principal (Residential & Administrative Services) in the first instance.

Notification of Data Held and Processed

All students, staff and other users are entitled to

- know what information is held and processed about them within the Northern College and why
- know how to gain access to it
- know how to keep it up to date
- know what is being done within the Northern College to comply with the obligations of the Data Protection Act

Responsibilities of Staff

All staff will be provided with a standard form of notification. This will state all the types of data that are held and processed about them, and the reasons for which they are processed. This will be done annually.

All staff are responsible for

- checking that information that they supply to the Northern College in connection with their employment is accurate and up to date
- informing the personnel department of any changes to information which they have provided, e.g. changes of address
- checking the information which will be sent out from time to time, as detailed above
- informing the personnel department of any errors or changes. The Northern College cannot be held responsible for any errors unless notification of those errors has been received

If and when as part of their responsibilities, staff collect information about other people, (e.g. about students' course work, opinions about their ability, references for students or other staff, or details of personal circumstances), they must comply with the guidelines for staff, which are at Appendix 1.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold are kept securely
- personal information is not disclosed either orally or in writing, 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 should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- when kept or in transit on portable media the files themselves must be password protected

Student Obligations

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

Students who use the computer facilities at the Northern College may, from time to time process personal data. If they do they must notify the Vice Principal (Residential & Administrative Services). Any student who requires further clarification about this should contact the Vice Principal (Residential & Administrative Services).

Rights to Access Information

Staff, students and other users of the Northern College have the right to access any personal data that are being kept about them either on computer or in manual files. Any person who wishes to exercise this right should complete the college 'Access to Information' form (see Appendix 2) and give it to the Vice Principal (Residential & Administrative Services). Any other member of staff receiving a request for access to personal data **must** pass on that request to the Vice Principal (Residential & Administrative Services), who will ensure that the 'Access to Information' form is completed and the request dealt with accordingly.

Where users are not either employees, students or members of the Board or Governors, the Northern College will make a charge of £10 on each occasion that access is requested – this is simply to cover the administrative costs of extracting the information. This charge can be waived at the discretion of the Vice Principal (Residential & Administrative Services).

The Northern College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days, unless there is good reason for delay. In such cases, the delay will be explained in writing to the person making the request.

Publication of Northern College Information

Alongside the Data Protection Act, the Freedom of Information Act 2000 gives a general right of public access to all types of recorded information held by "public authorities". The college falls under the definition of a public authority and is therefore covered by the Act. The college has a Freedom of Information Publication Scheme which is available through the Northern College website.

The FOI Act enables individuals to ask for information about any aspect of the college's work, however, requests for personal information should still be handled in line with the data protection guidelines.

Subject Consent

In many cases, personal data can only be processed with the consent of the individual. In some cases, if the data are sensitive, **express consent** must be obtained. Agreement to the processing of 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. The Northern 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. The college 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.

Therefore, all prospective staff and students will be asked to sign a Consent to Process statement, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

The Data Controller and Designated Data Controllers

The Northern College as a corporate organisation is the data controller under the Act, and the Board of Governors is therefore ultimately responsible for implementation. However, the designated data controller will deal with day-to-day matters.

The college's designated data controller is the Vice Principal (Residential & Administrative Services). In the absence of the Vice Principal (Residential & Administrative Services), any issue needing urgent attention relating to the provisions of this policy should be raised with the Principal, or other member of the Senior Management Team acting on her behalf.

Notification to the Information Commissioner's Office

The Northern College is registered with the Information Commissioner's Office as a data controller. This registration will be renewed annually and at renewal the data processing activities of the college will be reviewed to ensure that these match the activities that have been notified.

Use of CCTV

The college uses CCTV systems for the prevention and detection of crime and for protecting the security and safety of students, staff and other college users. The use of these systems is subject to the Northern College CCTV Code of Practice. This can be found as Appendix 3 of this policy.

Retention of Data

The Northern College will keep some forms of information for longer than others. The retention of data is governed in many cases by legislation. For employees this includes information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. For students this includes information necessary for the audit of funding claims. See Appendix 4 for a full list of information with retention times.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the Northern College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to college facilities being withdrawn, or in the most serious cases, a criminal prosecution. It can also lead to a significant fine being imposed on the college.

Appendix 1 – Guidelines for Staff

1. Data Collection

You must ensure that you only collect data for the purposes for which the college is registered. You should not create any data storage system (e.g. database, spreadsheet, computerised mailing list, or manual filing system) which holds personal data without the knowledge and permission of your line manager. Do not set up, or allow your staff to set up any of the above without checking the college's Data Protection Register entry first. You must also notify the Vice Principal (Residential & Administrative Services) of any new systems, or changes to existing systems for the processing of personal data, whether electronic or manual. The college is registered to hold data for the following tasks:

a) the provision of education, support and general advice services for our students and facilities to our clients

b) the promotion of the college and our services

c) the maintenance of our accounts

d) the support and management of our staff

e) the use of CCTV to maintain the security of our premises and for the prevention and investigation of crime

f) consultancy and advisory services

g) the conduct of research

h) the publication of college Newsletters and Magazines

If you are at all unsure as to whether what you want to do is covered, then either take a look at the full register entry, a copy of which is available online via the Information Commissioner's website, or contact the Vice Principal (Residential & Administrative Services). Please also get in touch if you feel that there are areas of the College's work which are not adequately covered.

You should also be aware that the obligations regarding the processing of personal data do not apply in cases where you may be processing data for your own personal or domestic purposes. An example of this might include personal contacts in your address book, lists of birthdays, etc.

2. Responsibility to Data Subjects

You must ensure that when you are asking for information, the supplier of that information knows what it will be used for. For example:

If you are collecting data on a form, include a sentence or paragraph which explains the need for the information, and who will have access to it. If you are asking for sensitive data, you must make sure that the subject signs to give 'express consent' for those pieces of data to be collected. If you are unsure about whether the information is sensitive, consult the Vice Principal (Residential & Administrative Services).

If you are collecting data by interview, or over the telephone, again ensure that you make clear at the start of the interview that the person that you are talking to understands why you are asking for the information, and what it is to be used for.

3. Sufficiency

Collect only as much information as is necessary. Be very clear about the intended use of the data, and restrict the data collection to that information which will allow you to carry out that task. If it is possible to avoid the use of 'personal data', i.e. to work with data from which individuals *could not be identified*, then this should be done.

Take every possible step to verify that the information that you are collecting is accurate. Where there are opportunities to check information, e.g. by cross-referencing with manual records, or by using tools within your software (spellcheckers, post-code verifiers) then take them. Your data should always be as accurate and up-to-date as possible.

Ensure that you have routines to correct any inaccuracies that come to light as soon as they are spotted. It is poor practice to leave data errors uncorrected, and in certain circumstances, can be disastrous, an erroneous digit in a payroll record for example.

4. Currency

Regularly review the data that you hold, and make sure that information is as up-to-date as possible. If your use of the data is ongoing, build in routines which will allow people to update the information that you hold on them. This can be as straightforward as asking people to notify you of a change of address.

5. Reports and Analysis

Make sure that any data processing, i.e. production of reports or statistical analysis, is done accurately, and in such a way that will not change or distort your source data. Do not expect untrained staff to carry out complicated statistical tasks, and ensure that **only** those who are entitled to see the information are responsible for working with it.

6. Retention

Do not hold information for longer than is necessary. The college must be able to justify the storage of any data, at any time. In accordance with statutory regulations, and college policy, archive where necessary, and delete data which is no longer of any use. DO NOT hold on to information just because you feel that it 'may come in useful' one day.

7. Disclosure

Data may only be disclosed to third parties in those cases where the Data Protection Act expressly permits disclosure. The transfer of data without consent may be permitted in the following circumstances:

- In the protection of the vital interests of the data subject (i.e. releasing medical data where withholding the data would result in harm to the data subject)
- For the purpose of preventing serious harm to a third party
- For the purpose of safeguarding national security
- For the prevention and detection of crime

- In the apprehension or prosecution of offenders
- In the assessment or collection of any tax or duty
- In the support of regulations such as securing the health, safety and welfare of employees

Only pass on information to those who are authorised to see or use it. Ensure that anyone from within the college requesting data has a bona fide need for the information, consistent with the purposes registered in the College's Register entry. If you are unsure as to whether you should disclose information internally, consult the Vice Principal (Residential & Administrative Services) for advice.

Never give information to an external enquirer without written proof of authorisation. Do not give details over the telephone, and ensure that your staff are aware of this restriction. If you believe that the enquirer has a legitimate right to receive information, and it is not practicable to delay disclosure, in the case for instance, of a police officer investigating an alleged criminal offence, please forward the query to the Vice Principal (Residential & Administrative Services). (The only exception to this is in the case of a genuine emergency, in which case information may be disclosed to the emergency services.)

Any person about whom information is held within a computerised or manual system in the college, has the right to see whatever information is being held, and to request that it be altered, should they regard it to be inaccurate. The college has a data access policy and a form, which anyone wanting to see their information should complete. Please refer anyone asking to see his or her data to the Vice Principal (Residential & Administrative Services).

8. Security

This is one of the most important aspects of data use, and the one to which all staff should pay close attention. Staff should ensure that where personal information is stored, care is taken wherever possible to restrict access to the data. It should not be possible for people walking in to an office, or walking past a computer screen, to read personal data. Similar care needs to be taken with the location and storage of printouts. Paper based systems containing personal data should be kept in locked drawers or filing cabinets.

Where it is necessary to transfer data to an approved third party, the transfer should be done as securely as possible. Data sent by e-mail, or saved on to data sticks, CDs or other similar media should be encrypted. Data sent in hard copy should be carefully addressed so that the opportunity for unauthorised access is minimised. Particular care should be taken with the use of fax machines to transmit personal data.

Computerised systems containing personal data should be fully password protected, the passwords changed regularly, and individuals made aware of the necessity to maintain the secrecy of their personal passwords. Users should make sure that unauthorised personnel are not able to read personal data from their computer screens.

Users of the network should use only their own login passwords, in order to maintain the security of the network system, and enable an 'audit trail', should the network's security be compromised. Computers that are not in use should be logged out or switched off. Offices containing computers should be kept locked when not in use.

Back-ups of data should be regularly carried out, and the back-up media held securely.

Personal data should be disclosed only to authorised personnel.

The long-term storage of college-related personal data off-site is subject to the prior approval of the Vice Principal (Residential & Administrative Services). Staff working on personal data at home should be aware of the security required for such data, and should ensure that unauthorised access is not given. College software and hardware should not be removed from college premises without prior authorisation. Where staff work on personal data at home, they must ensure that data held in manual form are stored as securely as possible, and ideally locked away. They must also ensure that any laptop or other personal machine that is used has an up-to-date firewall and anti-virus software.

Where employees take laptops or tablets containing personal data out of the College, the laptop or tablet must be kept secure. Whilst travelling the laptop or tablet should be constantly in view, and should not be checked into hold baggage.

Particular care should be taken in the use of smartphones, tablets or other portable devices which are capable of accessing college systems or other data sites such as web portals where personal data may be held. Any smartphone or tablet used for college work should be passcode protected to prevent unauthorised use.

Any perceived breaches of the security or loss of personal data held by the college should be reported immediately to the Vice Principal (Residential & Administrative Services).

9. Disposal of Data

All paper or microfilm documentation containing personal data should be securely shredded. All computer equipment or media that is to be sold or scrapped must have all personal data completely destroyed.

Appendix 2

Northern College for Residential Education

Access to Personal Information Request Form

Name:

Relationship to Northern College: Staff/Student/Governor/Other*
* delete as appropriate

If other please describe:

Please indicate below the information to which you wish to have access

1. Data that Northern College holds about me in the following categories:
    - Academic marks or course work details ☐
    - Academic or employment references ☐
    - Disciplinary records ☐
    - Health and medical matters ☐
    - Political, religious or trade union information ☐
    - Any statements of opinion about my abilities or performance ☐
    - Personal details including name, address, date of birth etc. ☐
    - Visual images e.g. from CCTV footage ☐

    or

2. All the data that Northern College currently has about me, either as part of an automated system or part of a relevant filing system ☐

Signature:

Date

Please return this form to the Vice Principal (Residential & Administrative Services). You may be asked to provide proof of your identity before information is released to you.

Appendix 3

Northern College

CCTV Code of Practice

Introduction

The purpose of this code is to regulate the management, operation and use of closed circuit television (CCTV) systems in the Northern College.

The system currently comprises a number of cameras located around the campus. Cameras are monitored from a number of locations including the office of the Children's Centre Manager, the ICT Technical Support Office, the college Reception and the LLSC. Any images which are recorded are only available to named officers of the College or partners with whom a data-sharing contract exists (see Annex A) and members of the Senior Management team who may be required to investigate any alleged incident. Sound is not recorded, with the exception of the system based in the Children's Centre office which covers that office only.

This code follows Data Protection Act guidelines.

The Code of Practice will be subject to review annually to include consultation as appropriate with interested parties.

The CCTV system is owned by the Northern College.

Objectives of the CCTV scheme

To protect staff, learners, visitors, children and property of the Northern College

To increase personal safety

Statement of intent

The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

The college will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

Cameras will be used to monitor activities within the Northern College to identify any untoward activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the staff and users of the college and safeguarding of its property and assets.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Recordings will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes to areas covered by the CCTV.

Operation of the system

The Scheme will be administered and managed by the Vice Principal (Residential and Administrative Services) or his/her deputy, in accordance with the principles and objectives expressed in the code.

The CCTV system will be operated 24 hours each day, every day of the year.

The Vice Principal (Residential and Administrative Services) or the named officers will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Access to the CCTV control equipment will be strictly limited to the named officers where essential maintenance is required and to members of the senior management team investigating any alleged incident.

Named officers must be present where monitoring equipment is based, or the rooms in which the equipment is sited must be locked.

Other administrative functions will include maintaining discs and hard disc space, filing and maintaining occurrence and system maintenance logs.

CCTV cameras used within the Northern College will be used in accordance with the following principles:

1. The system will produce clear images which law enforcement bodies can use to investigate crime and which can be taken easily from the system when required.
2. Cameras are sited so that they provide clear images
3. Cameras will avoid capturing the images of people not visiting the college premises
4. Signs indicating the use of CCTV cameras will be visible in those areas covered by the cameras
5. Recorded images will only be retained long enough for any incident to come to light and for that incident to be investigated.

Storage and disclosure procedures

In order to maintain and preserve the integrity of the media used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

Each item of media (e.g. CD or DVD) must be identified by a unique mark.

Before using each item of media must be cleaned of any previous recording.

The controller shall register the date and time of media creation including a reference.

A media item required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store. If a media item is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence store.

If the media item is archived the reference must be noted.

Media items may be viewed by the police for the prevention and detection of crime, and by the named officers for supervisory purposes, authorised demonstration and training.

A record will be maintained of the release of media items to the police or other authorised applicants. A register will be available for this purpose.

Viewing of media items by the police must be recorded in writing and in a log book. Media items will only be released to the police on the clear understanding that the

media item remains the property of the college, and both the media item and information contained on it are to be treated in accordance with this code. The college also retains the right to refuse permission for the police to pass to any other person the media item or any part of the information contained thereon. On occasions when a court requires the release of an original media item this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the college to retain the stored media items for possible use as evidence in the future. Such media items will be properly indexed and properly and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors) to view or release media items will be referred to the Vice Principal (Residential and Administrative Services). In these circumstances media items will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a court order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

Breaches of the code (including breaches of security)

Any breach of the Code of Practice by college staff will be initially investigated by the Vice Principal (Residential and Administrative Services), in order for her/him to assess the necessity for appropriate disciplinary action.

Complaints

Any complaints about the Northern College CCTV systems should be addressed to the Vice Principal (Residential and Administrative Services), who will deal with them under the Complaints procedure or the Employee Grievance procedure as appropriate.

Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access should be made on an Access to Personal Information Request Form available from the Vice Principal (Residential and Administrative Services).
The forms will also be available via the college website and intranet.

Annex A

Officers of the College permitted to view CCTV recordings:

LLSC: Library Staff, ICT Technical Support Staff

Children's Centre: Children's Services Manager, Senior Practitioner

Car Park: Reception Staff, ICT Technical Support Staff

General Areas: ICT Technical Support Staff

Long Barn Bar, Dairy: Elior Bar Staff

The Vice Principal (Residential and Administrative Services) as overall scheme manager will be permitted to view CCTV recordings for the purposes of the investigation of any alleged incident. In the absence of the Vice Principal (Residential and Administrative Services) another member of the Northern College Senior Management team will fulfil this role.

Appendix 4

Retention Schedule for Northern College

The table below lists the information that is currently recorded and kept by the Northern College, along with its period of retention, and location.

Record	**To be maintained by**	**Period of Retention**	**Location**
Minutes of the Board of Governors and its Standing Committees	The Clerk to the Governing Body	Historical record – kept in perpetuity	Clerk's Office Archive
Agenda, papers and other records of the Board of Governors	The Clerk to the Governing Body	10 Years – some historical documents kept in perpetuity for research purposes	Clerk's Office Personnel Archive
Published Financial Accounts	Head of Finance	Indefinitely	Finance Department
Financial Records including invoices, receipts, ledgers and accounts – hard copy and electronic	Head of Finance	7 Years	Finance Department
Payroll Data	Head of Finance	10 Years following cessation of an individual's employment	Finance Department
Tenders and Time-expired Contracts	Head of Finance	7 Years	Finance Department
External Funding Contracts	Head of Finance	Minimum of 7 years or in line with contractual requirements (e.g. ESF)	Finance Department
Internal and External Audit Reports	Head of Finance	7 Years	Finance Department
Employers Liability Certificate	Head of Estates & Facilities	20 Years	Estates Department
College Surveys	Head of Registry	7 Years	Registry Archive
Data Protection Registration	Vice Principal – Residential & Administrative Services	10 Years	Vice Principal – Residential & Administrative Services Office
Student Records – electronic and hard copy	Head of Registry	In line with ESF guidelines as updated annually (currently 31	Registry Archive

		December 2022	
Examination and Assessment Records	Head of Registry	Indefinitely	Registry Archive
Record	**To be maintained by**	**Period of Retention**	**Location**
Software Licences and Hardware Registers	Network Manager	5 Years	ICT Department
Copyright Clearance Records	Reprographics & Marketing Assistant	2 years for teaching materials For the duration of usage of web based materials	ICT Department
College Contacts Database	Public Relations & Marketing Officer	Database reviewed every 3 years	Business Unit
Student Advice and Guidance Records	Student Services Co-Ordinator	5 Years following cessation of an individual's enrolment	Student Services
Learner Support Fund Records	Additional Support Co-ordinator	7 Years	Student Services Finance Department
Confidential Student Counselling Records	College Counsellors	5 Years	Student Services
Quality System Files	Quality Manager	3 Years	QAC Office Archive
Staff Personal Files	Personnel Manager	Indefinitely	Personnel
Staff Professional Development Records and Files	Personnel Manager	5 Years	Personnel
Recruitment Files	Personnel Manager	6 Months from the date of the decision	Personnel
Sickness Absence Monitoring Records	Personnel Manager	2 years	Personnel
DBS Disclosures	Personnel Manager	6 months	Personnel
Accident Register	Health & Safety Officer	7 Years	Health & Safety Office Personnel
Health and Safety Records – including risk assessment, audits, PAT testing etc.	Health & Safety Officer	10 Years	Health & Safety Office
Records relating to occupational diseases and health, e.g. asbestos	Health & Safety Officer	40 Years	Health & Safety Office Personnel
Library Statistics and Membership Data	Head of Library, Learning	Maximum of 2 years following	LLRC

	Technologies and Student Support	cessation of employment or enrolment of borrowers	
Record	**To be maintained by**	**Period of Retention**	**Location**
Childcare Records	Children's Services Manager	3 Years following cessation of a child's placement in the Centre	Children's Centre
Line Management Files and Records	All Line Managers	Duration of individual's employment then forwarded to Personnel for disposal	Various
CCTV Footage	Network Manager	3 Months	ICT Department

Appendix 5 – Glossary of Terms

The Act - The Data Protection Act 1998

Data - Any information that will be processed or used within or by a computerised or manual system. This can be written, taped, photographic or other information

Data Subject - The person to whom the data relates

Data Controller - The person or organisation responsible for ensuring that the requirements of the Data Protection Act are complied with

Designated Data Controller - Individual appointed by the Northern College to carry out the day-to-day duties of the Data Controller

Manual System - Any paper filing system or other manual filing system which is readily structured so that information about an individual is readily accessible

Personal Data - Information about a living person that by itself, or in conjunction with other information which is kept in a manual or computerised system, is sufficient to identify an individual. This information is protected by The Act

Processing - Accessing, altering, adding to, changing, disclosing or merging any data will be processing for the purpose of the 1998 Act

Sensitive Data - Information about a person's religious beliefs, racial or ethnic origin, gender, trade union membership, political beliefs, sexuality, health or criminal record

Subject Consent - Before processing personal data, the College must have the agreement of the individual to do so. In the case of sensitive data, this must be specific consent, but in other cases, it can be more general

The Data Protection principles - the underlying principles of the Act that determine what data can be collected, processed and stored. A failure to abide by the principles will be a breach of the 1998 Act.

The Information Commissioner's Office - the body which enforces and oversees the Data Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations

The Data Protection Tribunal - The tribunal established to deal specifically with matters of enforcement under the Data Protection Act

Area	Data Protection
Sub Area	Personnel
Prepared By	Denise Pozorski
Approved By	Policy and Finance
Document Manager	Denise Pozorski

Last Updated	March 2015
Next Review Date	March 2018
Assessment Dates Where Appropriate	
Equality Impact Assessment	
Sustainability Assessment	
Safeguarding Assessment	