Peterborough Regional College

European Union
European Structural and Investment Funds

P104 Data Protection Policy

1. INTRODUCTION

This Data Protection Policy has been developed to ensure that Peterborough Regional College fully complies with the Data Protection Act 2003 and subsequent legislation.

This policy gives clear guidance and direction on the major issues of the Act in relation to an educational establishment such as Peterborough Regional College.

Furthermore, the policy emphasises the duties and obligations of every member of staff under the Data Protection Act 2003 and what the College sees as good practice.

Compliance with the 2003 Act is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, access to College facilities being withdrawn, or a criminal prosecution.

If there are any questions about the interpretation or operation of this policy, please contact the College Data Protection Officer.

2. PURPOSE

The purpose of this policy is to:

1. ensure that all staff and members of the College are fully briefed on data protection issues
2. inform staff of their responsibilities within the context of their job and show a line of responsibility towards implementing the Data Protection Act 2003 across the College
3. clarify the College's understanding of subject consent within the context of the Data Protection Act 2003
4. clearly define individual's rights with regard to processing personal data and accessing personal data within the context of the Act
5. give direction and guidance for dealing with requests to access personal data
6. ensure that all staff are fully briefed (or made aware) on the issues surrounding the disclosure of data
7. offer guidance on data retention periods and correct procedures for the disposal of data
8. ensure that Peterborough Regional College fully complies with the Data Protection Act 2003.

3. SCOPE

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 the College. Any failure to follow the policy can therefore result in disciplinary proceedings. Any member of staff or student, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the College Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

The College is not responsible for any personal data processed by a member of staff or a student for their personal or domestic use, even where this involves the use of College equipment. The definition of personal or domestic use covers any data not concerned with their employment or studies at the College.

4. RELATED DOCUMENTS

P106 Freedom of Information Policy
P505 Disciplinary Policy
P514 Providing Employment References
P600 Staff Internet & Email Policy
P601 Student Internet & Email Policy
P602 Information & Communications (ICT) Policy
P607 IT Security Policy
P608 Laptop Security Policy
P700 MIS Policy

5. RESPONSIBILITIES

The College, as a corporate body, is the Data Controller under the Act and the Corporation Board is, therefore, ultimately responsible for implementation.

A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for the College.

All departmental managers and all those in managerial or supervisory roles are responsible for developing and encouraging good practice with regard to the handling of information.

Compliance with data protection legislation is the responsibility of all members of the College who process personal information.

5.1 Staff

All staff are responsible for:

- checking that any information that they provide to Human Resources in connection with their employment is accurate and up-to-date

- informing Human Resources of any changes to information which they have provided i.e. change in address, telephone number, etc.
- checking the information that the College will send out annually, giving details of information kept and processed about staff.
- informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed Human Resources
- processing student data as requested in their job role in accordance with the Data Protection Act 2003.

5.2 Students 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 the Course Tutor who then must fill in the appropriate form. 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 their Course Tutor in the first instance.

5.3 Data Security

All staff are responsible for ensuring that:

- any personal data which they hold is kept securely
- personal information is not disclosed, whether orally, in writing, accidentally or otherwise, to any unauthorised third party. Section 8 of this policy, gives further detail on the disclosure of data.

Personal information should be:

- kept in a locked room, i.e. a locked staff room; or
- in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or kept only on a disk which itself is kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

This policy also applies to staff and students who process personal data off-site. Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the College campus.

5.4 Notification

The College has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Personal data must only be processed if the purpose for which it is required has been 'notified' to the Information Commissioner. It is a criminal offence to hold personal data that has not been registered.

A list of purposes, which have been registered by the College, is as follows:

Purpose 1	Staff, Agent and Contractor Administration
Purpose 2	Advertising, Marketing, Public Relations, General Advice Services
Purpose 3	Accounts and Records
Purpose 4	Education
Purpose 5	Student and Staff Support Services
Purpose 6	Crime Prevention and Prosecution of Offenders
Purpose 7	Provision of facilities to other groups or organizations
Purpose 8	Publication of the College magazine

Managers are expected to familiarise themselves with the terms of the College's register entry. If any doubt exists as to whether any particular collecting, holding and use, or intended disclosure of personal data is within the terms of the College's register entry or the Data Protection Act 2003, then staff must discuss this with the Data Protection Officer before taking action. Senior members of staff should keep the Data Protection Officer informed of non-standard data held in their areas.

Individual data subjects can obtain full details of the College's data protection register entry with the Information Commissioner from the College Data Protection Officer or from the Information Commissioner's website (www.dataprotection.gov.uk).

6. DEFINITIONS

Data - Any information, which will be processed or used on or by a computerised system. In addition, any information recorded as part of a 'relevant filing system' will be data. This can be written, taped, photographic or other information.

Data Subject – An individual who is the subject of personal data.

Personal Data – This is data about a living individual, who is identifiable by the data, or who could be identified by the data combined with other data, which the College currently has or may have in the future.

Sensitive Personal Data - Means personal data consisting of information as to the ethnic origin of the data subject, his or her political opinions, religion or creed, gender, trade union membership, political beliefs, sexuality, health or criminal record.

Processing - Accessing, altering, adding to, changing, disclosing or merging any data are defined as processing by the Act. (It covers almost anything, which is done with or to data.)

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 others, it can be more general.

Subject Access Request - This is a separate and formal procedure by which personal data are disclosed to the Data Subject.

7. EQUAL OPPORTUNITIES IMPACT ASSESSMENT

A Section 1 Equality Impact Assessment has been completed

8. DATA PROTECTION PRINCIPLES

All processing of personal data must comply with the eight Data Protection Principles of the Act. The Principles are based on the following three key concepts:

Purpose – personal data must only be held for a clear purpose or purposes.
Fairness – personal data must only be processed for legitimate purposes.
Transparency – data subjects must be given certain basic information about the personal data held about them.

The Eight Principles of the Act

I. Fairly and lawfully processed

'Personal data must be processed fairly and lawfully and in particular shall not be processed until certain conditions are met.' For example, the individual has to give consent to the collection and use of the data. Further, the 1998 Act distinguishes between 'ordinary personal data' such as name, address and telephone number and 'sensitive personal data' as defined above. Under the Act, the processing of sensitive personal data is subject to strict conditions.

II. Fair and lawful obtaining

'Personal data must be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.' For example, if the College is planning to disclose data to a third party, it should make this clear to the data subject at the outset, since failure to do so can be considered a breach of this Principle.

III. Adequate, relevant and not excessive data

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.' This means that the College must not collect more data than is necessary for the purposes that have been specified.

IV. Accurate and up-to-date data

'Personal data shall be accurate and, where necessary, kept up-to-date.' Where information is received about an individual and that information is supplied by a third party, then, wherever possible, steps should be taken to verify the accuracy of that information. Any individual who suffers damage because of inaccurate personal data held about him or her may be entitled to claim compensation from the College. Therefore, the College has a responsibility to make sure that all data held on an individual is accurate.

V. Not keeping data longer than necessary

'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.' For example, a disciplinary warning must be erased from the file once it is spent.

Retention periods for personal data and the standard minimum time limits that apply to Educational Institutions are included in Appendix 6. All staff should be aware of these time limits.

VI. **Processing only in accordance with the data subject's right** 'Personal data shall be processed in accordance with the rights of data subjects under this Act.' Data subjects have various rights under the Act, including the right to see any data held on them.

VII. **Taking of appropriate technical and organisational measures** '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.' Members of the College must, therefore, ensure that all data they are processing is safe and cannot be accessed by unauthorised persons or organizations.

VIII. **Transfer of information**
'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.' (Details of countries and territories that presently have an adequate level of protection, can be found on the Information Commissioners website.)

9. RISK ANALYSIS

This is Act is enforceable to the full extent of the Law. The risk to the College of not following the correct procedures is financial, reputational and may result in legal action against the college and/or staff by the authorities or private companies or individuals.

10. PROCEDURE

10.1 Subject Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The College understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists. It should be noted that explicit consent cannot be obtained by the presence of a tick box.

10.2 Internet

It is particularly important to obtain specific written consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe.

In most instances, consent to process personal and sensitive data is obtained routinely by the College (e.g. when a student signs an enrolment form or when a new member of staff signs a contract of employment). Agreement for the College to 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 posts or courses will bring the applicants into contact with children, including young persons between the ages of 14 and 19. The College has a duty under The Children's Act and other enactments to ensure that staff are suitable for the jobs 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. The College will only use this information in the protection of health & safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Sometimes it is necessary to process information about a person's criminal convictions, race and/or gender and family details. This may be to ensure that the College is a safe place for everyone, or to operate other college policies, such as the sick pay policy or equal opportunities policy. As this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, all new staff and students will be asked to give their written consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. Anyone with any concerns regarding this matter should speak to either the Executive Director of Human Resources, their Line Manager or the College Data Protection Officer.

10.3 Forms (Collecting Personal Data)

All College forms (whether paper-based or web-based) that gather data on an individual must clearly tell the person (data subject) what the purposes, uses and disclosures of the data will/may be. It may also be necessary to include information about any recipients of the data and what their use will be (i.e. same or different to the College).

10.4 Opting Out

The Act gives the data subject the right to 'opt out' of having their data used and, therefore, they must be given the opportunity to tick or click an 'opt out box' for future mail shots etc., should this be appropriate to the type of form they are completing. If an individual does not consent to certain types of processing (e.g. direct marketing),

appropriate action must be taken to ensure that the processing does not take place.

If any member of the College is in any doubt about these matters, they should consult the College Data Protection Officer.

10.5 Data Subjects' Rights

'Personal data shall be processed in accordance with the rights of data subjects under this Act.' (6th Data Protection Principle)

The Data Protection Act 2003 gives rights to individuals in respect of personal data held about them by others. The rights are: -

10.5.1 to make subject access requests regarding the nature of information held and to whom it has been disclosed

10.5.2 to prevent processing likely to cause damage or distress

10.5.3 to prevent processing for purposes of direct marketing

10.5.4 to be informed about mechanics of automated decision taking process that will significantly affect them

10.5.5 not to have significant decisions that will affect them taken solely by automated process

10.5.6 to sue for compensation if they suffer damage by any contravention of the Act

10.5.7 to take action to rectify, block, erase or destroy inaccurate data

10.5.8 to request the Commissioner to assess whether any provision of the Act has been contravened.

10.6 Rights of Access to Data (Subject Access Request) Staff, students and other users of the College have the right to access any personal data which are held by the College in electronic format and manual records which form part of a relevant filing system. Any individual who wishes to exercise this right should complete the College 'Subject Access Request' form.

The College will make a charge of £10 in accordance with the guidelines of the Data Protection Act 1998. 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 the delay will be explained in writing to the data subject making the request.

10.7 Examinations and Assessments (Subject Access Request)

10.7.1 Examination Scripts

Examination scripts are expressly exempted from the data subject access rules. This means that the College is under no obligation to permit examination candidates to have access to either original scripts or copies of the scripts.

10.7.2 Internal and External Examiners' Comments

Internal and external examiners' comments, whether made on the script or in another form that allows them to be held and applied to the original script or to a specific candidate (e.g. in an examiner's report or a coded table), are covered by the Data Protection Act 2003. A data subject has the right to request that a copy or summary 'in intelligible form' is provided within the stipulated timescale. This limit is normally 40 days. However in the case of examinations, the

Act specifically notes that such a request may be made before results are announced. Thus, there is a limit of five months from the request or 40 days from the announcement of the result, whichever is the earlier.

10.8 **References** (Subject Access Request)

Confidential information such as references may be disclosed under the Act. There are complicated rules relating to references, the subject of the reference cannot demand a copy from the person giving the reference, but, however, they could possibly obtain it from the person (or institution) receiving the reference.

Academic References

The writer of a reference may stipulate that it is confidential and he/she need not show it to the individual about whom it is written. However, once the reference is received, the subject of the reference may apply to the recipient for a copy. The recipient will have to balance any issues of confidentiality and any refusal of consent by the referee against the rights of the subject of the reference and, in many cases, the reference will be made available. Therefore, anyone preparing a reference should bear in mind that it may be seen by the person who is the subject of it. Writers of references should ensure that their references are accurate and that any opinions expressed are based on factual evidence. These principles also apply to internal references, reports and assessments for promotion and regrading.

10.9 **Right to Object to Data Processing** (Data Subject Notice)

Staff, students and other data subjects have a right to object to data processing that causes them damage or distress. Any member of staff, student or other data subject can serve notice prohibiting the College from processing data that can cause 'substantial damage or distress'. The College has 21 days in which to give evidence that they have complied or, instead, to give the reasons why they think that the individual's request is unjustified. (A data subject notice is only likely to be appropriate when the particular processing has taken place without justification and has caused, or is likely to cause, the data subject or another individual to suffer loss or harm or upset or anguish over and above the annoyance levels.)

10.10 **Automated Decision Making**

If requested, the College must be able to provide a formal statement that explains the logic behind any assessment based entirely on automated means. This includes single tests (e.g. multiple choice) that form only a part of some larger assessment and any classification or grading system that operates using automated means. Wherever possible, such information should be supplied to candidates before assessment, especially if the marking scheme involves non-apparent rules (such as the subtraction of marks for incorrect answers). Students have the right to demand (in writing) that no decision that significantly affects them is taken solely on the basis of automatic processing. Students are entitled to ask the College to manually review any marks generated solely by automatic means (such as optical mark reading).

10.11 **Disclosure of Data**

The College must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police. All staff

and students should exercise caution when asked to disclose personal data held on another individual to a third party.

In accordance with Principle 1 of the Data Protection Act 1998, personal data should only be disclosed if one of the conditions set out in Schedule 2 of the Act are met.

This policy, therefore, determines that personal data may be legitimately disclosed where one of the following conditions apply:

10.11.1 the individual has given their consent (e.g. a student/member of staff has consented to the College corresponding with a named third party)

10.11.2 where the disclosure is in the legitimate interests of the College (e.g. disclosure to staff - personal information can be disclosed to other
College employees if it is clear that those members of staff require the information to enable them to perform their jobs)

10.11.3 where the College is legally obliged to disclose the data (e.g. LSC returns, ethnic minority and disability monitoring)

10.11.4 where disclosure of data is required for the performance of a contract (e.g. informing a student's company or sponsor of course changes/withdrawal etc).

10.12 Consent Not Required

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

10.12.1 to safeguard national security*

10.12.2 prevention or detection of crime including the apprehension or prosecution of offenders*

10.12.3 assessment or collection of tax duty*

10.12.4 discharge of regulatory functions (includes health, safety and welfare of persons at work)*

10.12.5 to protect the vital interests of the individual; this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

10.13 Disclosures to the Police

Disclosures to the police are not compulsory except in cases where the College is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow the College to release information to the police without the consent of students or members of staff in limited circumstances. Such disclosures should only be made if the police confirm that they wish to contact a named individual about a specific criminal investigation and where the College believes that failure to release the information would prejudice the investigation.

The police must request the information from the College in writing. Staff are not obliged to release information to the police over the telephone. Most police forces will have their own request form, which should always include:

10.13.1 a statement confirming that the information requested is required for the purposes covered in Section 29 of the Act

10.13.2 a brief outline of the nature of the investigation

10.13.3 the data subject's role in that investigation

10.13.4 the signature of a senior officer.

Note.

If any member of staff is contacted by the police and unsure of how to deal with the request, please contact the Data Protection Officer or staff in the Security Office.

10.14 Disclosing Sensitive Personal Data

In accordance with Principle 1 of the Data Protection Act 2003, sensitive personal data should only be disclosed if one of the conditions set out in Schedule 2 and one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure of sensitive student data to third parties are:

10.14.1 the student has given their explicit (ideally written) consent

10.14.2 statutory obligation of the College (e.g. equal opportunities monitoring)

10.14.3 disclosure is in the vital interests of the student (e.g. information relating to a medical condition may be disclosed in a life or death situation).

Note.

Should a member of staff receive an enquiry as to whether a named individual is a member of the College, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (i.e. consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the College may constitute an unauthorised disclosure.

10.15 Disclosure of Examination Results

Examination results (including other forms of assessment such as coursework marks, module marks, phase tests) are personal data and, therefore, should not be disclosed to third parties without consent.

As the identity of the caller cannot always be confirmed, the risk of unauthorised disclosure of examination results over the telephone is high. Therefore examination results should never be released over the telephone.

10.16 Disclosure to the Media

The Information Commissioner's Office has produced an advice sheet, which provides guidance for Colleges who wish to disclose their students' examination results to the local media for publication. An outline of this note is provided in Appendix 4. Any Curriculum Area of the College wishing to disclose data in this way must follow the guidance of this note to ensure that any such disclosures are made within the remit of the Act. Publication of results on the Internet represents a transfer outside of the EEA and could potentially be in breach of Principle 8 of the Act. Explicit consent must be sought from students where it is intended to publish results on the Internet (opt-out is inadequate in this case).

Whatever method of disclosure is chosen, it is important to manage students' academic expectations carefully.

10.17 Retention and Disposal of Data

The College discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the College, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods

than others.

10.17.1 Student and Staff Files

All areas of the College should regularly review their files in accordance with the College's Records Retention Schedule in Appendix 6.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data i.e.

10.17.1.1 manual records should be shredded or disposed of as 'confidential waste'

10.17.1.2 electronic data must be appropriately deleted

10.17.1.3 hard drives of redundant PCs should be wiped clean before disposal. Further details on confidential waste disposal can be obtained from the College Technical Services Department.

11. CLOSED CIRCUIT TELEVISION (CCTV)

11.1 External Security Contractor

The campus has CCTV cameras placed in strategic positions and the responsibility for monitoring, recording and responding to the images is sub contracted to an independent security company, Business Watch. The operation of the cameras is covered by Business Watch's CCTV Code of Practice and Business Watch is the Data Controller in respect of the images captured. Data from this system is processed in accordance with the Data Protection Act 2003 and Business Watch's Data Protection Notification to the Information Commissioner.

11.2 CCTV Code of Practice

Business Watch's CCTV Code of Practice determines that:

- any monitoring of data will be carried out only by a limited number of specified staff
- data will be accessed only by the Security Manager and Security Control Room Operators from Business Watch and persons authorised by Business Watch in accordance with their Code of Practice.
- personal data obtained during monitoring will be erased as soon as possible after any investigation is complete
- data will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties
- staff involved in monitoring will maintain confidentiality in respect of personal data
- data are securely stored, where only a limited number of authorised persons may have access to them
- the operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment, such as the date and time stamp, are correctly set and applied to the data).

12. ACADEMIC RESEARCH

Personal data collected only for the purposes of academic research (includes work of staff and students) must be processed in compliance with the Data Protection Act 2003.

Researchers should note that personal data processed only for research

purposes receive certain exemptions (detailed below) from the Data Protection Act 2003 if:

- the data are not processed to support measures or decisions with respect to particular individuals and
- if any data subjects are not caused substantial harm or distress by the processing of the data.

If the above conditions are met, the following exemptions may be applied to data processed for research purposes only:

- personal data can be processed for purposes other than that for which they were originally obtained (exemption from Principle 2). However, as a matter of good practice, it is hoped that, wherever possible, researchers will contact participants if it is intended to use data for purposes other than that for which they were originally collected
- personal data can be held indefinitely (exemption from Principle 5)
- personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonymised (exemption from part of Principle 6 relating to access to personal data).

Other than these three exceptions, the Data Protection Act 2003 applies in full. The obligations to obtain consent before using data, to collect only necessary and accurate data, and to hold data securely and confidentially must all still be complied with.

Researchers must ensure that:

- as clear guidance as possible is provided to data subjects whose personal data will be used in research, as to why the data is being collected, and the purposes for which it will be used
- When processing involves sensitive personal data, explicit consent is gained and that data is held securely and confidentially so as to avoid unlawful disclosure.

13. PUBLICATION

Researchers should ensure that the results of the research are anonymised if published and that no information is published that would allow individuals to be identified.

APPENDICES

I. Subject Access Request (Guidance)

II. Subject Access Request (Examinations and Assessments)

III. Procedure and Form to make a Subject Access Request

IV. Disclosure of Examination Results by Schools/Colleges to the Media

V. Photographs (Guidance)

VI. Records Retention Scheme

VII. Forms:

- Consent for the use of photographs (Individual)
- Consent for the use of photographs (Group)
- Consent to retain exemplars
- Letter template for inviting candidates to collect their portfolio.
- Student Amendment

Appendix 1

Subject Access Request

Simple Requests

Whilst data subjects are entitled to request all the information that the College holds on them, it is likely that they are looking for something specific. Therefore, the majority of requests are likely to be from staff and students asking for copies of a specific document(s). These will usually be located from a single source - typically the staff/student files - and will not involve the disclosure of information relating to a third party. In such cases, College policy is to be open and transparent and, wherever possible, to let the individual have a copy of the information with minimum fuss.

When responding to such requests, staff must ensure that third party information is not inadvertently released without consent. No fee should be charged.

Complex Requests

There may be some instances when a request for information is more complex and will need to involve the College Data Protection Officer to ensure a co-ordinated response. It is hoped that such requests will be infrequent. Examples of situations where more complex requests might arise include:

- request involves locating information from multiple sources
- request involves the release of contentious information
- request is one in a series of requests from the same individual
- request involves the release of third party data for which consent has been refused or cannot be obtained
- the data subject does not want to ask for the information from the curriculum area/section that holds it.

In such cases, the appropriate procedure (Appendix 3) must be followed with the appropriate form filled in and passed to the College Data Protection Officer who will ensure that a co-ordinated approach is adopted and will determine whether or not it is appropriate to charge a fee. When responding to Subject Access Requests, the Data Protection Officer will liaise with staff in the Curriculum Area/Section as appropriate.

Third Party Data

It will sometimes be the case that responding to a Subject Access Request will lead to incidental disclosure of details relating to some other third party (for example, a referee or another student). Such third party information should not be disclosed without first seeking the consent of the third party.
If consent cannot be obtained (e.g. the third party cannot be contacted) or is refused, then the College needs to consider whether or not disclosure is reasonable, taking into account:

- any duty of confidentiality owed to the third party
- the steps taken to seek consent
- whether the third party is capable of giving consent
- any express refusal of consent.

If staff are unable to obtain consent, the College Data Protection Officer should be contacted. The Data Protection Officer will consider/balance the impact on the third party of the disclosure, and the impact on the data subject of the disclosure being withheld. Where third parties have been acting in an official capacity it may be argued that the duty of confidence is lower than is otherwise the case. However decisions will be made on a case by case basis. If the Data Protection Officer decides that disclosure cannot be made, only that information which could identify the third party should be withheld (e.g. third party details are blanked out). Wherever possible, the College will follow good practice by explaining to the data subject that some information has been withheld, and why.

Third parties who regularly supply information on students/staff in a professional capacity (external examiners, referees, etc) should be informed that anything they submit may become available to the data subject through a Subject Access Request. Curriculum Areas/Sections are advised to seek consent to disclose at the collection stage (e.g. when requesting references/appointing external examiners) to avoid delay upon receipt of a Subject Access Request. Where professionals request that information supplied by them be kept confidential, they must supply details of the exceptional reasons for making the request. The College will consider those reasons in order to decide whether they are valid.

College position on charging for Subject Access Request

The Data Protection Act 1998 permits organisations to charge up to £10 for responding to Subject Access Requests. However, this is unlikely to cover the costs of responding to requests, particularly when it involves locating information from numerous sources or where large volumes of information need to be photocopied and posted. There is no scope within the Act to charge more than £10.

Exemptions

There are certain situations where the College may not be obliged to release information in response to a Subject Access Request. Examples include:

- data containing information relating to a third party for which consent to release the information cannot be obtained
- examination scripts (although examiner comments must be released – see Appendix 2 Guidance on Examinations and Assessments for further information)
- management forecasts such as plans for redeployment, restructuring, promotions (if they would prejudice conduct of business/activity)

- information relating to legal proceedings being taken by the College against an individual.

Exemptions are an extremely complex part of the Act and must be treated with caution.

Appendix 2

Subject Access Request (Examinations and Assessments)

Under the Data Protection Act 1998, students have the right to request to see a copy of all information held on them by the College. This right extends to various documents/information collated during the examinations and assessment process.

Exam scripts

Exam scripts are specifically exempt from Subject Access Request provisions. This means that the College is not obliged to provide students with copies of exam scripts upon request.

Examiners comments (including external examiners comments)

Whilst exam scripts are specifically exempt from Subject Access Requests, comments made by examiners are not. This means that students are entitled to a copy of all comments made by both internal and external examiners. If comments are made directly onto the examination script, and the department chooses not to make the full script available upon request, the examiners' comments must be reproduced onto a separate form. It is, therefore, recommended that comments should be made on attached sheets, rather than directly onto examination scripts.

In all cases, examiners' comments must be provided to students in 'intelligible form' - this may mean providing a 'word processed' version if hand-written comments are potentially illegible.

All examiners should be reminded that their comments will be provided to students if requested and should, therefore, ensure that all comments can be justified and that no careless remarks are made on exam scripts, in emails/memos to colleagues, or on mark sheets. Any informal notes passed between examiners in the course of marking an examination script or piece of coursework should be disposed of securely once the final mark has been agreed and there is genuinely no need for the notes to be retained.

Results

If a student asks to see a copy of their results, the College must provide access to all examination/assessment marks either within 5 months of the request or 40 days after the official release of results (whichever is sooner). This extends to all students, regardless of whether or not they owe the College any money.

External Examiners' details

The College holds the names and addresses of all appointed External Examiners. This information is personal data and should, therefore, be processed in accordance with the Data Protection Act 1998. External Examiners should be adequately informed about the information held and for what purposes it will be used. Members of staff must not disclose names and addresses to third parties (i.e. outside the College) without the consent of External Examiners. External Examiners are entitled to make Subject Access Requests and, in particular, will be able to see emails and memos relating to views of staff about them. Therefore, staff should exercise caution when recording comments (includes email) about External Examiners.

External Examiners must be informed that any comments/marks/opinions expressed about individual students (during any stage of the assessment process) may be disclosed to the student upon receipt of a Subject Access Request. External Examiners must be advised that opinions expressed in a professional capacity will be disclosed to students if requested.

Appendix 3

Procedure for Subject Access Requests

Individuals wishing to access their personal information should submit a request in accordance with the following notes:

1. Make your request on the standard form (see below), to the Data Protection Officer.

2. The request should include details and provide documented evidence of who you are (e.g. driving licence, passport, birth certificate). You should also provide as much detail as possible regarding the information you wish to access (e.g. where and by whom information is believed to be held, specific details of information required etc).

3. You are not required to state why you wish to access the information: the details we require are merely those that will aid the efficient location and retrieval of information.

4. The College adopts a general policy of openness in terms of allowing individuals access to their personal information and, wherever possible, we aim to waive the £10 administration fee (permitted under the Data Protection Act 1998).

5. Once the Data Protection Officer receives a Subject Access Request, all efforts will be made to fully comply within 40 days. In any event, you will receive all the information that has been located and can be released within 40 days and an explanation for any information that cannot be provided at that time.

6. In accordance with the Data Protection Act 1998, the College does not usually release information held about individuals without their consent. Therefore, if information held about you also contains information related to a third party, the College will make every effort to anonymise the information. If this is not possible, and the College has been unable to secure the relevant consent, the College may decide not to release the information.

7. Should the request be made by a third party on behalf of an individual, the appropriate form (third party Subject Access Request form) must be filled in along with the standard request form.

All enquiries should be directed to the College Data Protection Officer in the first instance.

Contact Details of Data Protection Officer:

Name:	Peter Walker
Email:	peter.walker@peterborough.ac.uk
Postal Address:	Park Crescent Peterborough Cambs PE1 4DZ

Data Protection Act 1998

Standard Request Form for Access to Data (Subject Access Request)

(Personal data collected on this form will only be used for the above purpose)

Section A

FULL NAME (Block Letters) …….……

SIGNATURE ……..……...

STATUS (Delete as appropriate)

Current STUDENT/Former STUDENT (please give date last registered)…...……

……...

Course Details……

……...

Current STAFF/Former STAFF (please state date employment ceased)……..

Curriculum Area……..Payroll Number ……

National Insurance Number .....Maiden Name……...

If neither student nor staff, what relationship have you had with the College and when?

……...

HOME ADDRESS/ADDRESS TO WHICH DATA SHOULD BE SENT

……...

…….. POSTCODE ……..

TELEPHONE NUMBER …….

Both sides of this form must be completed and returned to: The Data Protection Officer, Peterborough Regional College, Park Crescent, Peterborough. PE1 4DZ

/CONTINUED

Section B

I, ……...(name) wish to have access to data that

the College has about me (please indicate as appropriate)

☐ course work details and grades
☐ employment references
☐ disciplinary records
☐ health and medical matters
☐ political, religious or trade union information
☐ personal details including name, address, date of birth etc
☐ other information (please describe the data you wish to see)

.....

……...

☐ If there is a specific document or data item you wish to see, please give as much detail as possible.

.....

……...

……...

I understand that I will have to pay a fee and provide proof of my identity.

Signed .....

Date .....
(You must complete sections A and B of this form and return to: The Data Protection Officer)

Section C (FOR OFFICE USE ONLY)

☐ Identification checked Date of acceptance
.....

☐ Fee received Last date for compliance ....….

Location of files	Date request forwarded	Date answer received

Data Protection Act 1998

THIRD PARTY SUBJECT ACCESS REQUEST FORM

1. Details of the third party requesting the information

Full Name .....……..

Address .....……...

.....……...

.....…… Postcode .....……..

Telephone Number.....……

NOTE: If you are acting on behalf of the Data Subject you must have their written authority to do so and you must enclose that authority with your request.

2. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.

.....…
..

.....……
..

……...

3. Details of the Data Subject

Full Name .....……..

Address .....……...

.....……...

.....…… Postcode .....……..

Telephone Number.....……

Note: All personal data collected on this form will only be used for the above purpose.

Appendix 4

Disclosure of Examination Results by Schools/Colleges to the Media The Information Commissioner's Office regularly receives enquiries about the data protection implications of Schools and Colleges disclosing their students' examination results to the local media for publication. This note explains how such disclosures can be made within the remit of the Data Protection Act 1998.

Basis for Processing

The Act requires that there should always be a legitimate basis for the processing of personal data. The Commissioner accepts that the publication of examination results takes places on the basis of a condition described in paragraph 6 of Schedule 2 of the Act, namely, where 'the processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason or prejudice to the rights or freedoms or legitimate interests of the data subject.'

Information to be provided to the pupils and parents

The Act also makes it clear that, in order for the processing of personal data, including its collection, to be fair, it is necessary to ensure that those to whom the data relate are aware of the purposes for which their data may be used or disclosed. While it is likely that many pupils/students and parents/guardians will be aware that examination results may be published, this is not always the case. To satisfy this requirement, therefore, Schools/Colleges should ensure that pupils/students and their parents/guardians are made aware that examination results may be published. It may also be necessary to explain the form in which publication will take place. Some pupils/students, for instance, might object to their results being published if they know that results are published in grade order rather than, say, alphabetically.

The Right to Object

Although the Commissioner does not think that pupils/students or their parents/guardians must give their consent to the publication of examination results, he knows from experience that, in a small number of cases, publication can cause distress. When informing pupils/students or their parents/guardians that examination results are published, Schools/Colleges should, therefore, advise them of the right to object to publication.

Pupils/Students or Parents/Guardians

The rights which the Data Protection Act 1998 gives data subjects are not affected by their ages. The Commissioner generally advises that as long as young people are able to understand their rights, then it is they, and not their parents or guardians, who should be informed of uses and disclosures of data and who have the right to object to processing. In most cases, therefore, it is sufficient to provide the information described above to pupils/students. In a small number of cases, it may be that pupils/students are not capable of understanding their rights or of understanding the consequences of

publication. In these cases, Schools/Colleges should provide the relevant information to parents or guardians.

Note. All external publications must have the consent of the College marketing team.

Appendix 5

Photographs (Guidance)

Visual images of individuals portrayed in photographs, where an individual can be identified, should be processed in accordance with the Data Protection Act 1998.

Under the Act, the data subject is responsible for deciding whether or not their photograph should be taken, provided they are able to understand their rights. And it is the responsibility of the member of staff involved to inform them why they want to take their photograph and how it will be used.

Note: 'Photograph' or 'Photography', includes digital and photographic prints, transparencies, video, film and other images i.e. mobile phone and/or webcams.

Individuals
Individual must be informed of the purpose(s) for which the photograph will be used and asked to give their consent. In most cases, verbal consent is all that will be required; however, there will be instances where written consent is necessary.

The following information should be obtained and retained with the photograph:

Member(s) of staff - Name(s) and Curriculum Area(s)
Student(s) - Name(s) and Course(s)
Purpose (e.g. where they will be printed and who will have access to them)
The date of the photograph should also be noted.

Organised Group
For an organised group (such as a class – either inside or outdoors) inform the class of the purpose for which the photograph is to be used and give the opportunity for individuals to opt out (i.e. temporarily leave the group). The date of the photograph and the identity of the group (e.g. Full Time Motor Vehicle Course) should be retained with the original photograph. If names are to be attached to the photograph written consent will be required.

If the photograph is just a group and does not focus on one individual (e.g. holding a trophy) then it could be argued that this is not personal data; however, it would still be good practice to request verbal consent.

Photographs taken for curricular, assessment, security, registration, training and development or travel reasons must not be used for any other purpose. With photographs now being used for assessment and the introduction of the electronic portfolio and the need for a third party to verify them, it is suggested that written consent is recorded.

Use of photographs for purposes other than those for which consent has been obtained.

An individual who poses for a photograph has, in effect, given their consent for that photograph to be taken. However, they may not fully understand how their image is going to be used which may result in distress and a claim for compensation. If the consent of an individual or group has been obtained for limited purposes and it is subsequently wished to use the photographs for another purpose (especially if the use is by an individual or body external to the College), the written consent of the individual(s) must be obtained.

Marketing

The marketing team are responsible for ensuring that students give written permission for their photograph to be used when covering stories for publicity. Where photographs are provided to the marketing team from other areas of the College, the photographer must ensure that he/she has written permission to use the image before passing this on to the marketing team. Under no circumstances must individual photographs be published externally without the consent of the marketing team.

Photographs of Children

The Information Commissioner's legal guidance states that, by the age of 12, a child is considered to have `sufficient maturity' to understand their rights under the Act. However, this is a complex issue and the College has, therefore, decided to adopt the following position: ‘for all students under the age of 16 (including all 14 – 16 IFP students) parental consent must be obtained in writing.’

Sensitivity

Sensitivity is as important in dealing with photography as it is in processing other personal data. Court cases have occurred because photographs have been used inappropriately. When using photographs or video footage, staff should be sensitive to cultural and religious beliefs. Although consent may have been obtained, care should also be taken as distress can be caused if a photograph or article appears alongside another unrelated article which could be considered offensive to the cultural or religious belief of the individual being portrayed.

Particular care should be taken in publishing photographs of individuals with physical, learning, communication or language disabilities as, although an individual may be over 18 years old, he/she could still fall under the scope of the Child Protection Guidelines.

Displaying Students' or Children's Artwork
Consent should be obtained to display artwork that would enable an individual (especially a child) to be identified and traced. If consent has not been obtained, the work should only include the first name. Care should be taken over any unusual names.

The Internet and World Wide Web
Photographs placed on the College's website and made available via the Internet on the World Wide Web will be available in countries which do not have a data privacy regime considered adequate by the EU Commission. It is, therefore, essential that written consent is obtained.

Award Evenings and Celebrating Success
Where photographs are likely to be taken at such events, it would be advisable to clearly state on the invitation form to the data subject or parent that photographs/video footage may be taken, and outline the purpose, requesting that the data subject or parent make contact with the College should they object. At such an evening, it would also be good practice during the welcome or introduction to announce that anyone who objects to having their photograph taken must indicate this to a member of staff.

Good Practice
Where verbal consent has been sought to take a data subject's photograph, good practice would indicate that a diary note of the request is made.

Disposal of photographs
Photographs must be confidentially destroyed or deleted from databases once they are no longer required for the purpose for which they were taken.

Appendix 6
Student Records

Type of record	Minimum retention period	Location	Reason for length of period
NVQ Programmes			
NVQ Records. This includes the minimum information required to track candidates' progress and to allow for the independent authentication of any claim. e.g. Assessment and IV records, date of registration, assessor and IV details. For most programmes this data is found in the NVQ Candidate Assessment Documents.	3 years	Curriculum Area	Joint Awarding Body Code of Practice requirement.
Candidate Portfolio (Assessment completed, full award gained)	Until seen by the External Verifier. After verification the course team should make every effort to return the portfolio to the candidate. A standard letter template is available (Appendix 7 – IV) to send to the candidate inviting them to collect their portfolio. The letter invites the candidate to collect their portfolio within three months otherwise the portfolio will be disposed of confidentially. Copies of all correspondence regarding collection of portfolios should be kept in the Course File.	Curriculum Area	Joint awarding Body Code of Practice requirement.
Candidate Portfolio (Assessment incomplete)	3 years The course team should make every effort to return the portfolio to the candidate. A standard letter template is available on the Corporate Intranet to send to the candidate inviting them to collect their portfolio. Copies of all correspondence regarding collection of portfolios should be kept in the Course File. If the candidate does not collect the portfolio it must be retained for a period of 3 years.	Curriculum Area	Joint awarding Body Code of Practice requirement.

Other Programmes/Courses			
Student records. This includes the minimum information required to track student progress and to allow for the independent authentication of any certification/award claimed. e.g. Assessment and IV/IM records.	1 year after certification.	Curriculum Area	Recommended good practice.
Assessed course work and student portfolios.	Until Certification. After certification the course team should make every effort to return the course work/portfolio to the student. A standard letter template is available (Appendix 7 - IV) to send to the student inviting them to collect their course work/portfolio. The letter invites the student to collect their course work/portfolio within three months otherwise it will be disposed of confidentially. Copies of all correspondence regarding collection of course work/portfolios should be kept in the Course File.	Curriculum Area	Recommended good practice.
Internal examination scripts from year 1. e.g. Edexcel phase tests/end tests.	Can be disposed of in year 2 (assuming it does not count towards the final mark for a unit or module being completed in year 2)	Curriculum Area	Relevant time to let students exercise their right of appeal or in case of any other dispute.
Internal examination scripts from year 2 onwards. e.g. Edexcel phase tests/end tests.	Duration of studies and 1 year after certification	Curriculum Area	Relevant time to let students exercise their right of appeal or in case of any other dispute.

General Records			
Exemplar course work / portfolio retention	Samples of coursework may be retained indefinitely in Curriculum Areas as exemplars only with the written consent of the author. (Standard form in Appendix 7.Ⅲ)	Curriculum Area	Consent required to avoid possible litigation.
Class record books	1 year	Curriculum Area	Good practice
Work placement records	1 year	VTU	Good practice
ADSUP records	Summary records 6 years. Individual records 2 years.	Curriculum Area	Recommended code of practice by the auditors
Sensitive information e.g. Dyslexia reports	At the discretion of the P.A.M.	Curriculum Area	To allow data to be consulted at a later date
Academic Appeals data	6 years from last action on case.	Curriculum Area	A limitation period for negligence
Disciplinary data	6 years from last action on case.	Curriculum Area/Learner Services	A limitation period for negligence
Records of enquiry and interview for students who subsequently enrol.	1 year	Curriculum Area	Good practice

Staff Records

Type of record	Minimum retention period	Reason for length of period
Personnel files including records and notes of any disciplinary and grievance hearings.	6 years	Reference and potential litigation.
Applicants details from recruitment process	1 year	Good practice
Wages and salary	6 years	Tax Management Act 1970
Facts relating to redundancies where less than 20 redundancies.	6 years	Time limit on litigation
Facts relating to redundancies where more than 20 redundancies.	12 years	Limitations Act 1980
Statutory Maternity Pay records and calculations	At least 3 years after the financial year to which records relate	Statutory Maternity Pay (General) Regulations1982
Statutory Sick Pay records and calculations	At least 3 years after the financial year to which records relate	Statutory Sick Pay (General) Regulations1982
Income Tax and NI returns including correspondence with tax office	At least 3 years after the financial year to which records relate	Income Tax (Employment) Regulations 1993
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; 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	3 years	Limitation period for personal injury claims
Medical records kept by reason of Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999

Appendix 7 - I

Consent Form (INDIVIDUAL)

Use of Photographs with the Data Subjects Name Added

I hereby consent to the use of my name and photograph, taken by a member of the College or by an agent authorised on behalf of the College, to use for the following purpose(s):

Purpose(s)

This photograph will not be used for any other purpose(s) than stated above and when spent will be confidentially disposed of. The supervision of this photograph and consent form will fully comply with the legislation of the Data Protection Act 1998.

Subject Name	
Course	
Tutor	
Photographer	

Subjects Signature…….. Date……..…..

Signature of Parent (If under 16 years of age)……...

Top copy: student
Second copy: course file

Appendix 7 - II

Consent Form (GROUP)

Use of Photographs with the Data Subjects Name's Added

We hereby consent to the use of photographs of ourselves, taken by a member of the College or by an agent authorised on behalf of the College, to use for the following purpose(s):

Purpose(s)

This photograph will not be used for any other purpose(s) than stated above and when spent will be confidentially disposed of. The supervision of this photograph and consent form will fully comply with the legislation of the Data Protection Act 1998.

Data Subjects Name	Course

Photographer	
Tutor	
Date	

Top copy: student
Second copy: course file
Appendix 7 - Ⅲ

Peterborough Regional College

CONSENT TO RETAIN EXEMPLARS

Samples of students' coursework, projects, portfolios, essays, dissertations, theses etc may be retained indefinitely in Curriculum Areas as exemplars only with the consent of the author.

I give my consent to Peterborough Regional College to retain the work specified below for an indefinite period of time as exemplar material. It has been pointed out to me how this material will be used and stored, and that the supervision of this exemplar material and my personal details, will fully comply with the legislation of the Data Protection Act 1998.

When the currency of this material is past the College will make every effort to return it to you or you may request its return at any point in time should you wish to do so.

Title	
First Name	
Surname	
Address	
Course	
Academic Year	
Exemplar Material	

Signed…… Date……

Top copy: student
Second copy: course file

Appendix 7 - IV

Tel (01733) 76 (Enter your extension number)

Student's Address

Today's Date

Dear (Student's Name)

_____Enter Name of Course_____

I am writing to you in connection with the above College course to advise you that your portfolio/course work is now ready for collection. The College will keep the portfolio/course work for three months from the date of this letter. If it has not been collected by then, the College will confidentially dispose of your portfolio/course work. Please note that, if you request a third party (family or friend) to collect the portfolio/course work on your behalf, your prior written permission will be required.

Yours sincerely

Enter tutor name.
Tutor