DATA PROTECTION POLICY

PURPOSE OF THE POLICY

The purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Yeovil College needs to keep certain information about staff, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the college must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 ("the Act"). The principles are set out in detail under the section *Data Protection Principles* later in this policy. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Not be kept longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The college and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the college has developed this Data Protection Policy. The policy applies to all staff and students of the college. Any breach of the Act or the college Data Protection Policy is considered to be an offence and in that event, Yeovil College disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the college, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

SCOPE

Definitions:

Personal Data: data relating to a living individual who can be identified from that information or from that data, and other information in the possession of the Data Controller. This includes name, address, telephone number and ID number. It also includes expression of opinion about the individual and of the intentions of the Data Controller in respect of that individual.

Sensitive Data: different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.

Data Controller: any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is processed and the way in which the personal data is processed.

Data Subject: any living individual who is the subject of personal data held by an organisation.

Processing: any operation related to organisation, retrieval, disclosure and deletion of data and includes: obtaining and recording data, accessing, altering, adding to, merging, deleting data retrieval, consultation or use of data disclosure or otherwise making available of data.

Third Party: any individual/organisation other than the data subject, the Data Controller (college) or its agents.

Recipient: any person to whom the data is disclosed, including another member of staff of the Data Controller.

Source: a recognised and lawful source of personal data collection.

Disclosure: a recognised and lawful recipient of personal data (in compliance with the purpose of processing).

Relevant Filing System: any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc from which the individual's information can be readily extracted.

Data: information which is:

- Being processed by means of equipment operating automatically in response to instructions given for that purpose.
- Recorded with the intention that it should be processed by means of such equipment.
- Recorded as part of a relevant filing system (a structured system).
- Forms part of an accessible record. This includes such things as manual index card files, microfiche etc

Data Protection Principles

All processing of personal data must be carried out in accordance with the eight data protection principles:

1. *Personal data shall be processed fairly and lawfully*. This means that in many cases, processing will not be allowed without the consent of the data subject (see "subject consent" below), or where the processing is required for the performance if a contract to which the data subject is a party, or necessary for compliance with any legal obligation which the Data Controller is subject. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the Data Controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. *Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes*. Data obtained for specified purposes must not be used for a purpose that differs from those.

3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held*. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data is given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. *Personal data shall be accurate and, where necessary, kept up to date*. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the college are accurate and up to date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the college of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of the college to ensure that any notification regarding change of circumstances is noted and acted upon.

5. *Personal data shall be kept only for as long as necessary*. This means that for as long as the college holds personal information, it must show a purpose for having them. If the college cannot justify keeping personal data it must get rid of them.

6. *Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act*.

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

8. *Personal data shall not be transferred to a country or a 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*. Data must not be transferred outside the European Economic Area (EEA) – the twenty-five EU Member States together with Iceland, Liechtenstein and Norway – without the explicit consent of the individual.

RESPONSIBILITY AND AUTHORITY

The college, as a corporate body, is the Data Controller under the Act.

A Data Protection Officer (the Vice Principal Resources) has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the college.

The Senior Leadership Team, Heads of Department and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the college.

Compliance with data protection legislation is the responsibility of all members of the college who process personal information. Members of the college are responsible for ensuring that any personal data supplied to the college are accurate and up to date.

<u>Status of the Policy</u>
It is a condition of employment that staff will abide by the rules and policies made by the college from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed
Notification is the responsibility of the Data Protection Officer.

All staff, students and other users are entitled to:

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

Responsibilities of staff
All staff are responsible for:

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

If and when, as part of their responsibilities, staff collect information about other people (eg about students' course work, opinions about ability, references to other academic institutions or details of personal circumstances), they must comply with the guidelines for staff (see Appendix A).

Data Subject Rights
Data Subjects have the following rights regarding data processing and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision-taking process that will significantly affect them.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

Student Obligations
Students must ensure that all personal data provided to the college are accurate and up to date. They must ensure that changes of address etc are notified to Registry/other person as appropriate.

Students who use the college computer facilities may, from time to time, process personal data. If they do they must notify the designated Data Protection Officer. Any student who requires further clarification about this should contact the designated Data Protection Officer.

Data Security

All members of staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party. All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or
- In a locked drawer or filing cabinet, or
- If computerised, password protected, or
- Kept on disks which are themselves 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.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

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.

Rights to Access Information

Staff, students and other users of the college have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college "Access to Data Request Form" at Appendix B (staff) and Appendix C (students) and hand it to the Data Protection Officer, although failure to complete the form does not invalidate the request.

For students, the college will make a charge of £10.00 on each occasion that access is requested, although the college has discretion to waive this. For staff, there will be no charge.

The college aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within twenty-one days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request. In any event, the 21 day period will not start until the college has received:

- all information reasonably required to identify the data subject;
- any fee due; and
- proof of identity.

Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Protection Officer who will take appropriate steps to make the necessary amendments.

The college has the right to refuse repeated or vexatious subject access reports under the Act.

Subject Consent

In many cases, the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained unless processing is necessary for one of the purposes stated in the Act. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a student on to any course,

and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of fourteen and eighteen. The college has a duty under the Children Act and other enactments to ensure that staff, students 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 the information in the protection of the health and safety of the individual.

Model Contract Clauses for staff contracts of employment are contained in Appendix D.

Disclosure of Data

The college must ensure that personal data is 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. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of college business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the college concerned.

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

- The individual has given their consent (eg a student/member of staff has consented to the college corresponding with a named third party).
- Where the disclosure is in the legitimate interests of the institution (eg 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).
- Where the institution is legally obliged to disclose the data (eg HESA and HESES returns, ethnic minority and disability monitoring).
- Where disclosure of data is required for the performance of a contract.

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

- To safeguard national security*.
- Prevention or detection of crime including the apprehension or prosecution of offenders*.
- Assessment or collection of tax duty*.
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)*.
- To prevent serious harm to a third party.
- To protect the vital interests of the individual, this refers to life and death situations.

*Requests must be supported by appropriate paperwork.

When members of staff receive enquiries 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 (ie 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.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the college may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer.
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally, ie "if the person is a member of the college" to avoid confirming their membership of, their presence in or their absence from the institution.

If in doubt, staff should seek advice from their Head of Department or the college Data Protection Officer.

Publication of College Information

It is college policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names of college governors and register of interests of governing body members and senior staff with significant financial responsibilities (for inspection during office hours only).
- List of staff.
- Photographs of Senior Leadership Team and college Governors.
- Information on examination results.
- Graduation programmes and videos or other multimedia versions of graduation ceremonies.
- Information in prospectuses (including photographs), annual reports, staff newsletters etc.
- Staff information on the college website (including photographs).

The college's internal telephone list will not be a public document.

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

It is recognised that there might be occasions when a member of staff, a student, or a lay member of the college, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the college should comply with the request and ensure that appropriate action is taken.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the college is a safe place for everyone, or to operate other college policies, such as the sick pay policy or equal opportunities policy. The college will not need such consent if processing is necessary for (a) complying with a legal obligation imposed on the college, (b) to keep an Equal Opportunity Policy under review where the data is about race or ethnic origin or (c) (in emergencies) protecting the data subject or a third party who cannot give consent. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students may be asked to give express 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. More information about this is available from the Data Controller.

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

Retention of Data
The college will keep some forms of information for longer than others. Because of storage problems and the requirements of the Act, information about students cannot be kept indefinitely, unless there are specific requests to do so. A list is attached; see Appendix E for the archiving guidelines and retention times employed by the college.

Direct Marketing
Any department that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes. Where the direct marketing is to be conducted by email or other electronic means, you must also ensure that it complies with the Privacy and Electronic Communications Regulations which is outside the scope of this Data Protection Policy. For further information contact the Data Protection Officer.

Use of CCTV
For reasons of personal security and to protect college premises and the property of staff and students, CCTV cameras are in operation in certain campus locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified staff.
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete.
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

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 1998.

Researchers should note that personal data processed ONLY for research purposes receive certain exemptions (detailed below) from the Data Protection Act 1998 IF:

- The data is 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).
- Personal data can be held indefinitely (exemption from Principle 5).
- Personal data is exempt from data subject access rights where the data is processed for research purposes and the results are anonymous (exemption from part of Principle 6 relating to access to personal data).

Other than these three exceptions, the Act 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.

Note to Researchers

Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes, the college hopes 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.

For those departments which gather sensitive personal data, extra care should be taken to ensure that explicit consent is gained and that data is held securely and confidentially so as to avoid unlawful disclosure.

Publication

Researchers should ensure that the results of the research are anonymous when published and that no information is published that would allow individuals to be identified. Results of the research can be published on the web or otherwise sent outside the European Economic Area but if this includes any personal data, the specific consent of the data subject must, wherever possible, be obtained.

Conclusion

Compliance with the 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 or access to college facilities being withdrawn or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the college Data Controller.

RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS

Tuition Fees Policy
Staff Disciplinary Procedure
Staff Contract
Code of Professional Conduct

Appendix A

YEOVIL COLLEGE
STAFF GUIDELINES FOR DATA PROTECTION

1. All staff are likely to process data about students on a regular basis. The college will ensure through registration procedures that all students give their consent to this sort of processing and are notified of the categories of processing, as required by the 1998 Act. The information that staff deal with on a day-to-day basis will be "standard" and will cover categories such as:

   - General personal details such as name and address.
   - Details about class attendance, course work marks and grades and associated comments.
   - Notes of personal supervision, including matters about behaviour and discipline.

2. Information which may also be held about a student's physical or mental health, sexual life, political or religious views, trade union membership or ethnicity or race is particularly sensitive and can only be collected and processed with the student's consent but great care must be taken to maintain confidentially at all times. Examples: recording information about dietary needs, for religious or health reasons, prior to taking students on a field trip; recording information that a student is pregnant, as part of personal duties.

3. All staff have a duty to make sure that they comply with the Data Protection principles which are set out in the college Data Protection Policy. In particular, staff must ensure that records are:

   - Accurate
   - Up to date
   - Fair
   - Kept and disposed of safely and in accordance with college policy.

4. The college's Data Protection Officer will designate staff in each area as "authorised staff". These are the only staff authorised to hold or process data that are:

   - Not standard data; or
   - Sensitive data.

   The only exception to this will be if a non-authorised member is satisfied that the processing of the data is necessary:

   - In the best interests of the student or staff member, or a third person, or the college, AND
   - He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

   This should only happen in very limited circumstances. Example: a student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's Witness.

   - Authorised staff will be responsible for ensuring that all data is kept securely.
   - Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the Data Protection Officer or in line with the college policy.

- Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated Data Protection Officer, or in line with college policy.
- Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information “standard” or is it “sensitive”?
- Has the notification of Personal Data and Consent to Process form been signed and returned? (This should be filed with the enrolment form if for a student).
- Are you authorised by the Data Controller to collect/store/process the data?
- Are you sure that the data is secure?

Appendix B
(for staff)

YEOVIL COLLEGE
ACCESS TO DATA REQUEST FORM

Standard Request Form for Access to Data

I _____ wish to have access to either (delete as appropriate)

1. All the data that the college currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that the college has about me in the following categories (please tick as appropriate):
    - Employment references
    - Disciplinary, grievance and capability 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
    - Other information: please list below

Signed _____ Date: _____

Appendix C
(for students)

YEOVIL COLLEGE
ACCESS TO DATA REQUEST FORM

Standard Request Form for Access to Data

I _____ wish to have access to either (delete as appropriate)

1. All the data that the college currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that the college has about me in the following categories (please tick as appropriate):
   - Academic marks or course work details
   - Academic references
   - Health and medical matters
   - Any statements of opinion about my abilities or performance
   - Personal details including name, address, date of birth etc
   - Other information: please list below

I understand that I will have to pay a fee of £ (fee of £10.00 per request payable).

Signed: _____ Date:_____

Appendix D

YEOVIL COLLEGE
CONSENT TO PROCESS – MODEL CONTRACT CLAUSES FOR STAFF

1. Data Protection

All staff are required to abide by the college Data Protection Policy, a copy of which is included in the Staff Handbook.

A failure to follow any of the guidelines in relation to the collection, keeping, processing or destruction of any personal data, whether regarding another staff member, student or other third party, and whether deliberate or accidental, will be regarded as potential misconduct, and may result in disciplinary proceedings being brought.

Deliberate or negligent misuse of data, whether by unlawful disclosure or otherwise, may be considered gross misconduct and may result in summary dismissal in the most serious cases.

2. Consent to Process

Staff agree, by virtue of this contract, to Yeovil College processing such information as may be necessary for the proper administration of the employment relationship, both during and after employment, provided that proper regard is had to such data protection principles as may be in force.

In particular, staff consent to any of the following information being processed for the purposes set out below:

- Membership of recognised trade union.
- Mental and physical health, including dates of absence from work due to illness and the reason for the absence.
- Matters relating to pregnancy and maternity leave.
- Criminal convictions.
- Race or ethnic origin.
- Qualifications.
- Matters of discipline, grievance and capability.
- Age and years of service.

This information may be processed for any of the following reasons:

- Payment of salary, pension, sickness benefit or other payments due under the contract of employment.
- Monitoring absence or sickness under an absence control or capability policy.
- Training and development purposes.
- Management planning.
- Negotiations with the trade union or staff representatives.
- Redundancy and succession planning.
- Curriculum planning and organisation.
- Timetable organisation.
- Compliance with Equal Opportunities Policy.
- Compliance with the Disability Discrimination Act.
- Carrying out checks through List 99 or other appropriate mechanisms eg Disclosure with Criminal Records Bureau.

3. Sick Pay

In order to administer the occupational sick pay and leave scheme, all staff are required to provide information about their absences and the reasons for it. In some cases, this will be

by way of self-certification. Any refusal to provide this information and consent to the college processing it will result in the college ceasing to pay further sick pay until the information is provided and the consent given. The college may, at its discretion, dispense with the need for consent to process in some circumstances.

Appendix E

YEOVIL COLLEGE
GUIDELINES FOR ARCHIVING DATA PROTECTION

Type of Data	Retention Period	Reason
HR files: training records; notes of grievance, disciplinary and capability hearings	6 years from the end of employment	Provision of references and limitation period for litigation
Staff Application forms: interview notes	6 months from the data of interviews	Limitation period for litigation
Facts relating to redundancies less than 20	3 years from the date of redundancies	Limitation period for litigation
Facts relating to redundancies 20 or more	12 years from the date of redundancies	Limitation period of litigation
Income Tax and NI returns: correspondence with Tax Office	6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	6 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Wages and salary records	6 years from the last date of employment	Taxes Management Act 1970
Records and reports of accidents	3 years after the date of last entry	RIDDOR 1985
Pension records	Indefinitely	Provision of information for Pension Authorities
Health Records	During employment	Management of Health and Safety at Work Regulations
Direct Debit Mandates	Indefinitely (at least 7 years)	Limitation period for refunds
Health Records where reason for termination of employment is concerned with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health	40 years	COSHHR 1994
Student Records including academic achievements and conduct	6 years from the last day of the course. 10 years with the consent of the student for personal and academic references	Limitation period for negligence

Policy Review				
Author Paul Bowe	Position Vice Principal Resources	Approved by Corporation/Committee Corporation	Approval date 14.11.13	Review date November 2015

Initial Equality Impact Screening

Have you consulted on this policy, service, strategy, procedure or function? Yes
Details: HR, Finance, Registry

What evidence has been used for this assessment?

Could a particular group be affected differently in either a negative or positive way? Indicate Y where applicable

Group	**Negative impact**	**Positive impact**	**Evidence**
Age			
Disability			
Gender (incl. Transgender)			
Race (incl. Gypsy &Traveller)			
Religion or belief			
Sex			
Sexual orientation			
Marriage & civil partnership			
Pregnancy & maternity			
Other groups (see guidance)			

If any negative impacts are identified, are there any related polices, services, strategies, procedures or functions that need to be assessed alongside this screening? If yes, please detail below:

Should the policy proceed to a full Equality Impact Assessment? No
If no, please give reasons
The policy does not affect any grouping either negatively or positively.

Declaration
We are satisfied that an initial screening has been carried out on this policy and a full Equality Impact Assessment is not required.

We understand that the Equality Impact Assessment is required by the College and that we take responsibility for the completion and quality of this assessment

Completed by: PAUL BOWE Position: VP Resources Date: 7th November 2013

Checked by: PAULA BROWN Position: Director of HR Date: 7th November 2013