Abertay University
Secretariat

Data protection policy

Author	University Secretary
Approved By	Court
Approval Date	18 June 2014
Review Date	2019
Version	1.4
Document Type	Policy
Activity/Task	Information and knowledge management/Policy, guideline and procedures, legislative compliance
Document Location	

Version Control Table

Version number	Purpose / Changes	Author	Date
1.0	Approved by Court	Uni Secretary	2002
1.1 Draft	Proposed updates incorporated by University's legal advisers and Deputy Uni Secretary. Submitted to FPGP in May 2009	Thorntons/DUS	2008/2009
1.2 Draft	Change suggested by FPGP incorporated and submitted to Court for approval	DUS	June 2009
1.3 Approved	Updated with details of Court approval and to amend role titles	DUS	June 2009
1.4	Review and revision to take account of changes in roles and practice – draft for discussion	University Secretary/Compliance Office	March 2014

C O N T E N T S

1. POLICY STATEMENT

1.1 The policy of the University of Abertay Dundee (“the University”) is to comply fully with the requirements of the Data Protection Act 1998 ("the Act"). The University will operate procedures in accordance with the eight principles specified in the Act, i.e. personal data held by the University shall:

(i) be obtained and processed fairly and lawfully;

(ii) be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes;

(iii) be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed;

(iv) be accurate and, where necessary, kept up to date;

(v) be held no longer than is necessary for the purpose(s) for which it was collected;

(vi) be processed in accordance with the rights of the data subjects under the Act;

(vii) be surrounded by proper security;

(viii) not be transferred outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of the data subject.

The University and all staff and others who process or use any personal data must ensure that they follow these principles at all times, irrespective of (i) where the personal data is held and (ii) the ownership of electronic equipment used to process personal data, for the purposes set out in this policy. The conditions in the Act applicable to the processing of personal data are set out in Appendix 2.

[Note: other policies, developed by Abertay University’s Information Services, cover the use of personal and portable electronic devices on the University’s network, and also the use of the ‘cloud’.]

1.2 The University will register as a Data Controller with the Information Commissioner and will notify the Information Commissioner of:

(i) the personal data being or to be processed;

(ii) the category or categories of personal data subject to which they relate;

(iii) the purposes for which the personal data are being or are to be processed;

(iv) the people to whom the University may wish to disclose the personal data;

(v) the names, or a description of any countries or territories outside the European Economic Area to which the University may wish to transfer the personal data; and

(vi) a general description of security measures taken to protect the personal data.

1.3 Responsibilities for ensuring the University's full compliance with the Act are as follows:

(i) The University Secretary has direct responsibility for personal data protection within the University.

(ii) The Registrar has specific responsibility for student personal data issues.

(iii) The Director of HR and Organisational Development has specific responsibility for staff personal data issues.

(iv) Individual Schools/Services will nominate a representative to:

- liaise with the Secretariat as appropriate for guidance on personal data protection issues

- seek to ensure, as far as possible that the personal data processed by their School/Service is in accordance with the University's Data Protection registration, is not excessive for its purpose, is securely maintained and is kept up to date.

(v) All staff and students have a responsibility to comply fully with the requirements of the Act.

Disciplinary Offence

All staff and students should be aware that unauthorised access to, use, or disclosure of personal data or failure to comply with any of the provision for security of such personal data will be considered by the University as a disciplinary offence and action will be taken in accordance with the University's Staff Disciplinary Procedure or Student Disciplinary Code (as applicable) [available from the University Intranet and/or the Secretariat of the University].

2. PURPOSES OF PROCESSING, PERSONAL DATA SUBJECTS, CLASSES OF PERSONAL DATA AND EXTENT OF DISCLOSURE

2.1 For the Administration of Education and Training

2.1.1 Purposes of Processing

In order to enable the University to provide a continuing service to its student population, the University must obtain and retain certain personal data relating to individuals. The purposes for which the University will use this personal data are listed below, but the personal data may, in addition, be used for associated purposes. It is a duty of all staff members that they ensure that personal data relating to individuals is not used for purposes other than those listed below without first notifying the University Secretary of such intended use. The purposes for which personal data will be used are:

(i) to enable the University to administer student related functions and services from original enquiry and application through to graduation and alumni services thereafter;

(ii) to plan and account for the use of the services provided;

(iii) to produce information including statistics for agencies such as the Scottish Further & Higher Education Funding Council (SFC), and the Higher Education Statistics Agency (HESA.

(iv) to enable University staff to identify and communicate with students both on- and off-campus while enrolled at the University and after leaving;

(v) to monitor academic progress over a period of time towards qualification;

(vi) to carry out assessment and authorise awards;

(vii) to monitor freedom of information requests, complaints, disciplinary cases and academic appeals, including the use of external organisations or services to detect plagiarism or other forms of academic deceit;

(viii) to communicate information relating to University activities and functions;

(ix) to inform alumni of the University of matters which may be of interest to them;

(x) to arrange, facilitate and manage student placements or academic exchanges for purposes including work experience, training, teaching and learning, or research;

(xi) to share information with other bodies, including for example the Open University under the “Back on Course” agreement with Abertay University, for the purpose of providing individual students who have withdrawn with impartial advice and guidance;

(xii) for student computer software in the Library and computer laboratories to video/stills of students when sitting unsupervised examinations, tests and/or assessments on University computers for the purposes of

ensuring that the examination regulations are complied with, and that work done on computer under controlled conditions is students' own;

(xiii) to confirm qualifications to actual or potential employers as part of a reference or equivalent employment-related enquiry;

(xiv) to provide membership or other benefits to students from professional, or accrediting bodies;

(xv) to facilitate voluntary surveys of student opinion, related to the assessment and enhancement of the student experience and the performance of the University;

(xvi) to monitor use of the ICT facilities (as defined in the University's Regulations governing the use of University information and communications technology (ICT) facilities ("Regulations"), including internet use, for the purposes of:

- establishing the existence of facts and to ascertain compliance with these and other University Regulations;
- to prevent or detect crime;
- to investigate or detect unauthorised use of information and communications technology systems;
- to ensure effective system operation;

all in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000 as amended. (Please revert to the University's Web Filtering Policy and Regulations for further information – available from the University Intranet and/or the Secretariat of the University).

- For sensitive personal data, the University may request consent to process this information, or it may do so to protect the vital interests of students (in terms of Condition 3 of Schedule 3 to the Act) and also in connection with litigation; for the prevention of crimes such as fraud; and for health purposes, for counselling, and for the review of information for the purposes of the Equality Act 2010.

- Monitoring of the protected characteristics of staff members is undertaken under pursuant to Condition 2(1) of Schedule 3 to the Act, because it is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

2.1.2 Personal Data Subjects

The data subjects are primarily enquirers, applicants, students (current and former) and relatives, guardians and associates of the aforementioned data subjects. However, the University may also hold personal data relating to advisers, consultants and other professional experts, authors, publishers,

editors, artists and other creators, staff (including volunteers), giftors, agents, temporary and casual workers, suppliers and third parties participating in coursework.

2.1.3 Classes of Personal Data

The personal data the University collects about data subjects is both of a personal and sensitive nature and consist of the following:

(i) Details of telephone enquiries, including the following personal data:

Name and address, telephone number, area of interest, source of information, age, special need or disability.

(ii) Details from the University application form or UCAS application form[1], including the following personal data:

Names and addresses, age, gender, nationality and country of residence, area of permanent residence, educational records to date, academic references, special needs or disabilities.

(iii) Further personal data collected at enrolment or updated during a student's time at University or following graduation. This personal data includes the following:

Home address and next of kin, ethnic origin, sexual orientation, gender identity, faith or belief, address whilst attending University, University entry and other qualifications, demographic information, funding and fee related details, course and stage details, attendance, work experience, qualifications, academic progress and current status, assessment results, final results, student photographs, first employment destination. In addition, contact preferences and information of note set out by the individual, in response to an annual mailing requesting information, which is related to keeping in contact with the University after graduation.

(iv) The University may collect further personal data where required to or where the student has contact with specific support services within the University. This personal data may include the following:

Membership of Students' Association, medical details, record of contacts with counselling service, disciplinary details.

(v) Personal data will be collected from the University's ICT monitoring systems and this will include:

Web site visited with day/time, computer login sessions, computer processor and disk utilisation, security audit trails, network loading and e-mail volume.

(vi) Personal data will also be collected *via* the University's monitoring of landline telephone calls. The personal data may include:

[1] *When applying via UCAS, applicants are invited to read and agree to a declaration that UCAS and the universities and colleges to which application is made can process personal information and keep a copy of an application to collect statistics and to detect and prevent fraud*

Fully itemised reports including number called, time of call, duration of call and location of call.

2.1.4 Disclosures

Access to all student personal data within the University, whether on paper, computer files or other storage media, is controlled and restricted to those who are authorised by the University to access such personal data. By accepting the University's Registration Data Protection Statement (see Appendix 1 of this Policy), the data subject agrees to the disclosure of his/her personal and sensitive personal data in the following instances and subject to Section 3 of this Policy:

(i) to University staff, and the staff of partner institutions where appropriate, who need the information for administrative, teaching, assessment, recruitment or quality assurance purposes (please see Section 3: Transfers of Data outwith the European Economic Area, below);

(ii) to the Students' Association with respect to providing students' addresses and programmes for members of the Students' Association and for those new students expected to enrol;

(iii) to BIS SFC, HEFCE, HESA and other governmental agencies for statistical purposes;

(iv) to governmental (including the Home Office or successors to the UKBA); accrediting; regulatory, statutory, or professional bodies in connection with registration, membership, benefits, professional activities, continuing professional development and standards, and awards;

(v) to bona fide research workers, if approved by the Registrar or the University Secretary;

(vi) to the University's insurers, legal advisers and debt collection agencies;

(vii) to Local Education Authorities, SAAS, Student Loan Company, or other sponsors or funding bodies, in connection with grants, fees, student loans, and debt recovery;

(viii) where the University is subject to a court order;

(ix) to callers in emergencies and subject to the conditions in Note 1 below;

(x) to the Police, subject to the conditions in Note 2 below;

(xi) to Jobcentre Plus or successor organisation as required by the Social Security Administration Act 1992 or successor legislation;

(xii) to Local Authorities in respect of council tax and electoral roll enquiries;

and additionally, in the case of specific information on a student's progress and attendance, only in the following cases:

(xiii) to University staff for teaching, examination or assessment purposes;

(xiv) in confidential references in connection with applications for employment or further education;

(xv) to LEAs, SAAS and the Student Loans Company in connection with grants and fees;

(xvi) to employers or others formally sponsoring students in connection with attendance and progression; and

(xvii) information on the final award gained by each student will be published in the local and national press unless the student explicitly does not consent to this when asked on registering to graduate, and

(xviii) to external organisations or services, whether online or otherwise, to detect plagiarism or other forms of academic deceit.

OUR POLICY REGARDING DATA PROTECTION APPLIES EQUALLY TO ENQUIRIES FROM PARENTS.

Notes:

1. *In the event of an enquiry in an emergency where, in our judgement, it is in the student's interest to disclose personal data and where it is not possible to obtain the student's consent, the University may agree to provide the minimum necessary details to assist the enquirer, having first confirmed their credentials.*

2. *Where the Police are investigating a criminal offence in which a student may be involved or where the University is of the reasonable opinion the Police should be made aware of the activities of a student, the matter will be passed to the University Secretary or other senior manager as designated by the University Secretary for a decision on the release of personal data.*

2.1.5 Responsibilities

(a) The University will

(i) set up and maintain student records promptly and accurately on receipt of enquiry, application, enrolment and amendment details;

(ii) safeguard the privacy of individual students by a strict nondisclosure policy;

(iii) comply with all legal provisions in protecting all personal data on computers or in other formats from unauthorised access or use as set out in Section 4 of this Policy;

(b) In order to help us maintain meaningful records students (current and former) should:

(i) provide accurate personal data at application and enrolment;

(ii) inform the University, via the web-based self-service student records interface (or otherwise if appropriate) promptly about any changes (for example to their name or address) affecting our records;

(iii) notify the University, via the web-based self-service student records interface (or otherwise if appropriate) promptly of any changes to their programme of study which have been agreed by the relevant academic staff; and

(iv) notify us promptly in writing if they intend to withdraw from study either temporarily or permanently.

2.2 Staff, Agent and Contractor Administration

2.2.1 Purposes of Processing

In order to enable the University to fulfil its obligations as an employer, to comply with best practice in human resource management and to properly account for and control our activities, the University must obtain and retain certain personal and sensitive personal data relating to individual employees. The purposes for which personal data will be used are as follows:

(i) to enable the University to discharge its legal responsibilities as an employer, including responsibilities in respect of the payment of all amounts due in respect of employment, statutory deductions, and other deductions as authorised by individuals;

(ii) to enable the University to plan and account for the use of its resources and of the services provided;

(iii) to provide information including statistics for agencies such as the Scottish Further & Higher Education Funding Council and the Higher Education Statistics Agency;

(iv) to enable members of University staff to identify and to communicate with each other whilst in the employment of the University;

(v) to manage, and to monitor, complaints and disciplinary cases;

(vi) to monitor use of the ICT facilities (as defined in the University's Regulations governing the use of University information and communications technology (ICT) facilities ("Regulations"), including internet use, for the purposes of:

- establishing the existence of facts and to ascertain compliance with these and other University Regulations;
- to prevent or detect crime;
- to investigate or detect unauthorised use of information and communications technology systems;
- to ensure effective system operation;

all in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000 [Please revert to the

University's Web Filtering Policy for further information - available from the University Intranet and/or the Secretariat of the University].

2.2.2 Personal Data Subjects

The Data Subjects relevant to our processing in connection with the administration of staff, agents and contractors are, on the whole, staff of the University including volunteers, agents, temporary and casual workers and the relatives, guardians and associates of the aforementioned. However, in connection with this purpose we may also hold personal data on advisers, consultants and other professional experts, agents and contractors, customers and clients, and previous and prospective employers of the main data subjects.

2.2.3 Categories of personal data held

Our files and databases include the following categories of personal data:

(i) details of applications for employment with the University including such personal data as: name and address, email address, date of birth, telephone number, position applied for, gender, nationality, special need or disability, educational records to date, history of previous employment, employer references;

(ii) personal data collected at employment with the University including personal data such as: national insurance number, bank account details, membership of a pension scheme, membership of a trade union, next of kin, history of pay awards and incremental awards, details regarding, location within the University, University internal extension number, University email address, contract details, details of performance review, minutes of meetings, details of disciplinary and grievance procedures, specific job responsibilities, timetabled teaching hours, research publications, medical details;

(iii) personal data collected from the University's web filtering system and this will include: network session connection times, computer processor and disk utilisation, security audit trails, network loading and e-mail volume; and

(iv) personal data collected *via t*he University's monitoring of telephone calls; the personal data collected will be itemised communication bills including number called, duration of call, location of call.

(v) for the purposes of the Equality Act 2010, monitoring of the protected characteristics, including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, gender, and sexual orientation.

2.2.4 Disclosure

Access to all personal data of staff within the University, whether on paper, computer files or other storage media, is controlled and restricted to those who are authorised to access such personal data in the context of the University's official business. By accepting the terms and conditions of employment, staff members agree to disclosure of their personal and sensitive personal data in the following instances:

(i) in relation to contact details, to other University staff who need the personal data for the purpose of carrying out their duties within the University;

(ii) to BIS, SFC, HEFCE, HESA and other governmental agencies for statistical purposes;

(iii) to the University's insurers and legal advisers;

(iv) where the University is subject to a court order;

(v) to callers in emergencies and subject to the conditions in Note 1 below;

(vi) to the Police, subject to the conditions in Note 2 below; and

(vii) in confidential references in connection with applications for other employment or further education.

Notes:

1. *In the event of an enquiry in an emergency where, in our judgement, it is in the staff member's interest to disclose personal data and where it is not possible to obtain the staff member's consent, the University may agree to provide the minimum necessary details to assist the enquirer, having first confirmed their credentials.*

2. *Where the Police are investigating a criminal offence in which a staff member may be involved or where the University is of the reasonable opinion that the Police should be made aware of the activities of a staff member the matter will be passed to the University Secretary or a senior manager as designated by the University Secretary . for a decision on the release of personal data*.

2.2.5 Responsibilities

The University will

(i) set up and maintain payroll and personnel records promptly and accurately on receipt of employment details;

(ii) safeguard the privacy of individual staff members by a strict non-disclosure policy; and

(iii) comply with all legal provisions in protecting all personal data on computers or in other formats from unauthorised access or use.

In order to help the University maintain meaningful records, staff members must:

(i) provide accurate personal data on employment;

(ii) inform the HR Office promptly about any changes (for example to their name or address) affecting the University's records.

2.3 Use of CCTV

2.3.1 Purposes of Processing

The University has installed closed circuit television systems throughout its campus properties. This system is in place to assist with the maintenance of security, including the security of users of our premises and to assist with the prevention and detection of crime.

2.3.2 Personal Data Subjects

The University's CCTV systems may hold images of students, staff, visitors and other individuals who are physically present within the University campus or in the immediate vicinity of University premises.

2.3.3 Categories of Personal Data held

The University's CCTV systems record images, date and time. CCTV images are automatically retained for thirty days after which their contents are overwritten.

2.3.4 Disclosure

CCTV images will not normally be viewed unless an incident is reported.

The circumstances under which the University (its Security staff or senior management only) would view the personal data held on its CCTV systems are as follows:

(i) to identify individuals who have entered or exited from the premises following reports of any incidents;

(ii) to provide additional evidence in the investigation of any incidents which occur on or around University property;

(iii) to assist the Police with the prevention and detection of crime where a specific request is made by them;

(iv) a record of the details of, and the reason(s) for, any disclosures will be made in Security's incident log, and

(v) the University will, exceptionally, consider requests to release images to a third party on a case-by-case basis, where the needs of the third party outweigh those of the individual(s) whose images are recorded.

2.3.5 Responsibilities

The University will ensure that the use of CCTV cameras is signalled by the positioning of appropriate notices.

2.4 Research

2.4.1 Purposes of Processing

The University may process personal details in connection with academic research or statistical analysis in all fields including scientific, technical, health, social, economic or market research. This processing may include the identification of subjects for survey or analysis, the collection or extraction of personal data, the analysis, interpretation and evaluation of personal data, the output/presentation of results or findings and the administration of research funding.

2.4.2 Data Subjects

In connection with processing for the purposes of research, Data Subjects will be the subjects of that research, but may also be advisers, consultants and other professional experts, correspondents and enquirers, financial sponsors, customers and clients, relatives, guardians and associates of the other Data Subjects, staff including volunteers, agents, temporary and casual workers, and students and pupils.

2.4.3 Categories of Personal Data held

When data is stored for research purposes, the norm is that the data will be stored in an anonymised fashion. However, a specific research programme may require that records on individuals held in connection with research may include all categories of personal data, including sensitive personal data. In such circumstances it would be normally be the case that consent for this would be sought from all research participants.

2.4.4 Disclosure

Personal data held on individuals in the context of research may be disclosed to other members of the research team for the purposes of conducting that research but will not otherwise normally be disclosed without appropriate steps being taken to anonymise individual personal data.

3. TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA

The University will not transfer personal data outside the European Economic Area ("EEA") except in the following circumstances:

(i) In respect of personal data relating to students enrolled at the University but based at premises managed by institutions outwith the EEA who have a partnership arrangement with the University, the University will transfer personal data to the partner institutions.

(ii) In respect of University staff based at premises managed by institutions outwith the EEA who have a partnership arrangement with the University, the University will transfer personal data to the partner institutions.

(iii) Such transfers as are mentioned in the two paragraphs above will be undertaken in compliance with the Eighth Data Protection Principle: "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."

4. SECURITY MEASURES

4.1 Physical Security

The University takes very seriously its obligations in terms of the Act. The University Secretary has overall responsibility for the security of personal data throughout the University, although individual Schools/Services also share that responsibility.

The University will review the risks represented by the processing of the personal data and will, in each case, implement a level of security appropriate to those risks. All security measures which are imposed will be evaluated against the potential risks and the cost, effectiveness and practicability of the proposed levels of security.

It is the responsibility of all students and staff to ensure that any person whose identity is unknown is refused access to areas where personal data is held and all unescorted visitors and unauthorised personnel are to be restricted from areas where personal data is used.

Where personal data is held solely on an automated system, the University will ensure that there is a suitable back-up for that personal data.

Where the University in its discretion deems it to be appropriate, certain personal data may be de-personalised, coded or encrypted with a secure key. Such measures will be taken where the University deems the personal data to be of a critically sensitive and personal nature or where its disclosure would represent a real security risk.

The University will also ensure that reasonable access control mechanisms are put in place, including, where appropriate, the use of passwords, encryption, compartmentalised access and access logs, to enable the University to track unauthorised use of personal data.

Where it is necessary for the University to disclose personal data to third parties, such disclosure will be made with regard to the Seventh Data Protection Principle: "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."

All other aspects of information security, including but not limited to the methods, devices, and locations used for processing data; the related audit and monitoring of data processing, and the retention and destruction of records, are covered by policies related to this which are managed by Information Services and by Registry, copies of which are available on the University's intranet.

The University does not encourage the processing of personal data outwith the University's premises. There is, potentially, an increased risk of loss, theft or damage of personal data where this is done off premises. Where laptop computers or personal machines do require to be used in other locations, then reasonable precautions should be made to ensure that the personal data is not accessed, disclosed or destroyed and that any personal data held in manual form is stored as securely as possible and locked away when not in use. In addition, any person using personal data outwith the University's premises should ensure that up to date scanning programmes have been installed on laptop computers and all disks, emails and other potential virus carriers

are scanned regularly. If there are any security incidents, they should be reported immediately to the University.

The University shall regularly review the security arrangements which are put in place and where necessary shall notify the appropriate personnel of any changes to those security measures.

4.2 Audit Procedures

To ensure that all personal data kept by the University is accurate, up-to-date and is held for no longer than necessary, the University intends to carry out regular audits of the personal data held on individuals at least once every three years. If the University becomes aware that any personal data which is held is excessive or out-of-date, then it will take all reasonable steps to destroy that personal data as quickly as possible. Such personal data will be destroyed in accordance with the security provisions noted below.

4.3 Monitoring Procedures

The University will regularly review the use to which personal data collected by it is put. This will ensure that any additional notification which requires to be given to the Information Commissioner shall be accurate. All members of staff will require to notify the Secretariat of any uses of personal data which are not currently covered by the University notification.

4.4 Destruction of Personal Data

Where there is a risk of personal data being destroyed, where it is not intended to do so, the University shall ensure that there is a workable disaster recovery mechanism in place and that there are provisions for frequent back-up or duplicate copies of all personal data produced to be safely stored in a location wholly separate from that of the primary personal data source. In addition, the University has designated the Head of Information Services with the responsibility of ensuring the recovery of personal data and establishing its accuracy and integrity, within a reasonable time-scale following any disaster.

If personal data does require to be destroyed, the minimum standard which the University requires for the destruction of paper and microfilm documentation is shredding. If the personal data is stored in electronic format, then this should be reformatted or overwritten to ensure that nobody can access that personal data.

5. RIGHT OF ACCESS

Under the Act, individuals have a right to request and receive a copy of all personal data of which he or she is a subject. The University has a right to charge a fee of £10 to answer any personal data request.

The University will endeavour to comply promptly - and certainly within the 40-day time limit specified by the Act - to all such data subject access requests upon receipt of a request in writing accompanied by payment of the relevant fee.

Before releasing any personal data under a subject access request the University has an obligation to satisfy itself that the person requesting the personal data is in fact the data subject. All data subject access requests should therefore be passed to the University Secretary for authorisation.

In terms of the Act, students do not have an automatic right to view examination scripts. The University reserves the right to refuse access to any of its students to view either their original exam scripts or copies of the scripts.

However, all students do have the right to see any comments made by either internal or external examiners and, if requested, copies will be produced by the University within the normal 40-day time scale, on payment of a fee where appropriate. In line with this policy, all members of staff should ensure that any comments made on scripts are accurate and appropriate.

6. POLICY UPDATES

This Policy may be updated from time to time. Any updates will be highlighted in the University's Intranet page and it is your responsibility to review the latest version.

APPENDIX 1

STUDENT ON-LINE REGISTRATION DATA PROTECTION STATEMENT

Before you can become fully registered you must read and accept the following:

Data Protection

The University of Abertay Dundee will process your personal data and sensitive personal data. on its manual and computerised systems for the purposes of administering your education, associated financial matters, use of the University facilities and where appropriate, accommodation. Sensitive personal data includes, for example, information about physical and mental health; racial/ethnic origin.. Some personal data will be disclosed to third parties such as to the Higher Education Statistics Agency:

http://www.hesa.ac.uk/index.php?option=com_content&task=view&id=141&Itemid=171

Government Education Departments, Funding Councils, University of Abertay Dundee Students' Association and similar organisations. Full details of the University's Data Protection policy are available on the University Intranet or from the office of the University Secretary. Your acceptance of Registration is your consent to the University processing your personal data (including your sensitive personal data) in accordance with the University's Data Protection Policy. If you do not wish your personal data to be processed as specified in the Data Protection Policy, you are required to submit formal notification to the University. However, you should be aware that even if you do submit such formal notification, the University may be under a legal obligation to process your personal data as specified in the Data Protection Policy. Your acceptance below is also your consent to submit any form of assessment provided by you to a plagiarism detection service.

University Regulations

Full copies of all University policies, rules and regulations are available on the University intranet or from the office of the University Secretary.

Declaration

I hereby undertake to accept and abide by all policies, rules and regulations of the University, whilst I am an enrolled student of the University. I undertake to pay all relevant tuition fees if such fees are not received from a sponsoring body. I further consent to the University processing the personal data which I have provided to the University in accordance with the University's Data Protection Policy.

Please click ACCEPT REGULATIONS to continue: