MANCHESTER METROPOLITAN UNIVERSITY

DATA PROTECTION POLICY

This policy should be read in conjunction with the Data Protection Guidance, which is attached as:
Appendix A – Dealing with Personal Data
Appendix B – The Use of Personal Data in Research
Appendix C – Dealing with Students' Personal Data

1 INTRODUCTION

1.1 Purpose of Policy

To provide guidance on the use of personal information and to ensure that the University complies with the Data Protection Act 1998.

1.2 Scope

This policy and guidance applies to all University staff, students and others who use or process any personal information.

1.3 Roles and responsibilities

The Board of Governors is ultimately responsible for implementation of the policy; however, the Data Protection Officer is responsible for day to day matters. Any member of staff or student wishing to make specific enquiries about their data should, in the first instance, contact the Data Protection Officer at the Legal Department.

1.4 Aims of the Act

The University must comply with the Data Protection Act 1998 (the Act), which requires that data is collected and used fairly, stored safely and not processed unlawfully. The Act sets out the Data Protection Principles. In summary, these state that personal data shall:

1. be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
2. be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;
3. be adequate, relevant and not excessive for those purposes;
4. be accurate and kept up to date;
5. not be kept for longer than is necessary for those purposes;
6. be processed in accordance with the data subject's rights under the Act;
7. be kept safe from unauthorised access and processing, and accidental loss, damage or destruction;
8. not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The main aim of the Act is to provide individuals with some control over the use of their personal data, in particular, unforeseen secondary uses; and protection from unwanted or harmful uses of the data. The intention is to ensure that personal data is collected and used responsibly. In order to achieve this aim, the University must apply the following key concepts:

- Purpose – personal data should be processed only when there is a clear purpose for doing so.
- Fairness – individuals must be informed of the purposes for which their data is to be processed; and processing must meet one of a number of criteria set out in the Act, for example, that it is necessary in order to pursue the legitimate interests of the University. There may be legitimate interests for processing personal data even where the individual may not wish this to happen.
- Transparency – as individuals are responsible for enforcing their rights, they need to know the purpose of the processing and the measures the University has taken to ensure that processing is fair.

2 UNIVERSITY AS DATA CONTROLLER

The University needs to collect and process personal data (information about its staff, students and other individuals who come into contact with the University). The University is the registered data controller under the Act and has notified the Information Commissioner that personal information may need to be processed for specific purposes, listed in the University's registration under the Public Register of Data Controllers on the Information Commissioner's Office (ICO) website. The registration can be viewed by entering 'Manchester Metropolitan University' in the search box.

The register provides details of the **purposes** for which personal information may be used; types of data subjects about whom personal information may be held or processed; types of personal information that may be processed; bodies to whom the University may **disclose** information; and information about transfers of personal information.

3 PERSONAL DATA

Personal data is defined by the Act and relevant case law. It includes any information in the University's possession (or likely to come into its possession) by which a living individual can be identified (directly or indirectly). It may include photographs; videos; and expressions of opinion or indication of the University's intentions in respect of the individual. It also includes both data processed by computer or internet software and data recorded and processed manually as part of a filing system.

Sensitive personal data

Sensitive personal data can only be collected and processed in certain limited circumstances, set out in Schedule 3 of the Act. One of the conditions listed under Schedule 3 **must** apply in order to process sensitive personal data. The most commonly applied Schedule 3 condition is the express (written) consent of the data subject (person to whom the information is about).

The meaning of 'sensitive personal data' is defined by the Act and relevant case-law. In summary, it consists of information as to the data subject's: racial or ethnic origin; political opinions; religious (or similar) beliefs; trade union membership; physical or mental health/condition; sexual life; the (alleged) commission of any offence by the data subject, and associated proceedings or sentence of any court.

Sensitive personal data may be processed to ensure that the University is a safe place for everyone, or to operate University policies, such as the sick pay or equal opportunities policy. Offers of employment or course places may be withdrawn if an individual refuses to consent to the processing of their sensitive data, without good reason.

4 STAFF AND STUDENT RESPONSIBILITIES

4.1 Staff & student responsibilities

Compliance:
Staff who collect or process information about other staff or students in the course of their duties (eg course work, opinions about ability, references from external bodies, details of personal circumstances) must comply with this policy and guidance.

Any student who collects and processes personal data as part of their course or studies must comply with University policy and the Data Protection Act.

Heads of Department are responsible for ensuring departmental compliance with this policy and guidelines and shall actively promote compliance to their staff.

Security and confidentiality:
Staff and students must ensure that personal data is kept securely and is not disclosed to any unauthorised third party. Staff and students must not take personal data off-campus unless it has been deemed absolutely necessary by their Head of Department/Tutor. If it is necessary to take personal data off-campus, appropriate safeguards for ensuring the security of personal data must be taken, proportional to the risks presented in processing the data. It should be noted that the Information Commissioner has the power to fine the University for

accidental losses of personal data and that individuals may be prosecuted for more serious or deliberate breaches of the Act. Measures should be taken to prevent unauthorised or unlawful processing; accidental loss or destruction; or damage to personal data. See section A4 of the Guidance for practical advice on data security.

Staff or students who discover a potential or actual security breach must immediately inform the University's Legal Department; for example, finding a memory stick holding unencrypted personal data.

Subject access requests:
Subject access requests received by staff must be forwarded immediately to the Legal Department. Staff asked by the Legal Department to provide data, for the purpose of responding to a subject access request, must respond promptly, to ensure that the University meets its statutory deadlines.

Own personal data:
All staff and students are responsible for checking that information they provide to the University in connection with their employment/studies is accurate and up to date. Any changes to personal data provided (eg change of address) must be promptly notified, in writing, to the University (via the Faculty Office for students). The University cannot be held responsible for errors unless the member of staff or student has properly informed the University about them.

4.2 Others (eg contractors / consultants)

Third parties such as consultants, contractors or agents, undertaking work on behalf of the University involving personal data, must adhere to the University's Data Protection Policy and guidance and comply with the Data Protection Act. Provision will be made in contracts with external providers, consultants, etc, to ensure compliance with this Policy and the Act. Where third parties undertake work on behalf of the University, the University remains the data controller of all personal data.

5 RIGHTS OF DATA SUBJECTS

5.1 Right of Access to Information

Subject to the terms of the Act, staff, students, and other data subjects of the University, are entitled to know what information the University holds and processes about them and why; how to keep it up to date; and how to gain access to that information. This is known as a subject access request ('SAR'). Any person wishing to exercise this right should complete the University's Access to Information (Data Protection) form for staff/students/other data subjects (also

available from the Legal Department and from Faculty Offices) and submit this to the Legal Department.

The University will make a charge of £10 for each SAR received, as permitted under the Act.

The University aims to comply with SARs as quickly as possible, and within the 40 days allowed by the Act, unless there is good reason for delay; in which case, the reason for delay will normally be explained in writing to the applicant. The 40 day deadline starts to run only when the written request, proof of identity **and** £10 fee are received. The deadline may be suspended if it is necessary for the University to seek clarification or further information from the applicant, until such time as the clarification/information is received by the University.

5.2 Right to Object to Data Processing

Individuals have a right to object to data processing that causes them unwarranted and substantial damage or distress. Any person who wishes to register an objection must do so in writing, by letter, addressed to the Legal Department, specifying exactly what data processing they object to and why this will cause (or is causing) unwarranted and substantial damage or distress. The University will determine what is appropriate in the circumstances, with reference to the Act and ICO guidance, on a case by case basis.

6 RE-USE OF PERSONAL DATA

The University may process personal data, for academic research purposes (where there is benefit to the researcher and/or University). Research involving sensitive personal data (such as ethnicity or health) requires explicit (written) consent from the data subjects prior to processing. Researchers and supervisors are responsible for ensuring compliance with the Act and the University's Data Protection Policy and guidance.

Personal data collected and held by the University for another purpose may be processed by staff for research purposes, without further consent from the data subject, under s33 of the Act; and where the processing is necessary for the purposes of the legitimate interests of the University, under the fair processing condition, paragraph 6, Schedule 2 of the Act. Such processing is allowed, provided that it does not support measures or decisions regarding individuals and does not (nor is likely to) cause substantial distress or damage to any data subject. Personal data processed under s33 of the Act may be kept indefinitely and data subjects have no right of access to the data processed provided that results do not identify individuals.

Research results will not lead to decision making about individuals or groups of individuals and may be published or shared with a third party, provided that no individual can be identified.

7 COMPLIANCE

Compliance with the Act and this policy is the responsibility of all members of staff and students. It is a condition of employment that employees will abide by the rules and policies made by the University. It is a condition of being a student that all University rules and policies are fully complied with.

Any breach of the policy by a member of staff or student may result in disciplinary action or access to the University's facilities being withdrawn. Serious or deliberate breaches of the Act may result in a criminal prosecution.

Any breach of the Act by the University may result in a substantial fine or sanction imposed upon the University by the ICO.

8 FURTHER INFORMATION

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer in the Legal Department. Any individual who considers that the Policy has not been followed in respect of personal data about themselves, should raise the matter with the University's Legal Department.

Further information about the Data Protection Act 1998 can be found on the Information Commissioner's Office (ICO) website.

Please see the policy section of the MMU website for related policies.

Version	2.0	Author Name & Job Title	Sara Shanab Head of Legal Department
Approved Date	25 Nov 2011	Approved by: (Board/Committee)	Board of Governors
Date for Review	25 Nov 2016		

MANCHESTER METROPOLITAN UNIVERSITY
DATA PROTECTION GUIDANCE

Note: 'data subject' is the individual to whom the personal information relates.

APPENDIX A – DEALING WITH PERSONAL DATA

A1 DISCLOSURE OF DATA

Staff must not disclose personal data to anyone, except as required within the course of their duties. Unauthorised disclosure may be a disciplinary matter. Staff must not disclose personal data orally or in writing, accidentally or otherwise, to any third party. Note that confirming whether or not an individual is a student or employee of the University is a disclosure of personal data. All requests for disclosure of personal data should be referred to the Data Protection Officer in the Legal Department.

The University, as Data Controller, must decide whether or not to disclose information to third party enquirers, with reference to the individual circumstances, the Act and current guidance from the ICO. Except in cases of emergency, the enquirer should be asked to make a request in writing, which should be referred, to the Legal Department, before a response is given. **Emergencies** should be referred immediately to the Legal Department.

Third parties include: the police, family and friends, the media, local authorities and government bodies (unless for purposes listed within the registration above), bailiffs and other persons wishing to serve writs or enforce court judgements in civil matters.

The University's entry on the Public Register of Data Controllers on the ICO website contains full details of individuals and organisations to whom personal information may be shared with or disclosed to. The University may disclose certain limited information about its staff and students to the following **for specific purposes only** (this is not a definitive list):

A1.1 Staff

- relevant government departments and other bodies to whom we have a statutory obligation to release information, including:
  - Department for Education and Skills
  - Higher Education Statistics Agency (Fair Processing Notice)
  - Inland Revenue
  - Department of Social Security
- potential employers of our staff;
- potential providers of education to our staff;
- external agents employed by the University in the conduct of its business.

A1.2 Students

- relevant government departments and other bodies to whom we have a statutory obligation to release information, including:
  - HE/FE Funding Councils
  - Higher Education Statistics Agency (Fair Processing Notice)
  - Quality Assurance Agency
  - Student Loans Company
  - Local Education Authorities
  - Local Authority Council Tax Offices
- Manchester Metropolitan University Students' Union [MMUSU];
- libraries of higher education institutions participating in the North West Consortium [NoWAL];
- current or potential employers of our students;
- current or potential providers of education to our students;
- students' sponsors/funding bodies;
- students' former schools/colleges, for University marketing purposes;
- external agents employed by the University in the conduct of its business.

A1.3 Restrictions on disclosure

Disclosures to persons or institutions not listed within the Register will be made only with the permission of the data subject, unless exceptional circumstances apply, as provided by law.

A2 CHECKLIST FOR PROCESSING DATA

Before processing personal data, consider the following:

- Is it necessary/essential to record the information?
- Has the data subject been told that this type of data will be processed?
- Is the information factual, sufficient but not excessive, fair and accurate?
- Do you have the data subject's consent to process?
- Will the University be able to justify processing the data if asked to do so? [Processing must be fair, lawful, and meet at least one of the conditions under Schedule 2 (and, for sensitive personal data, Schedule 3) of the Act].
- Is the data 'sensitive' [see section 3 of the Policy]?
  - If yes, contact the Legal Department for advice.
- Are you sure that the data can be kept confidential and secure and only for as long as is necessary?

If you are asked for access to personal data by the data subject:
The University recognises that staff and students may occasionally require access to some types of personal data held on file about them. The procedure for making a Subject Access Request is outlined in Section 5.1 of the Policy. However, in practice, the University would not generally expect a member of staff or student to submit a formal SAR, and pay a £10 fee, for example, for a copy of a single, standard, document from their personal file. This information may only be released if it is not confidential and does not contain any personal data about any third party (anyone other than the person making the request). The identity of the data subject must be verified before releasing any data.

If there is **any doubt** as to whether or not the information should be released, contact the Legal Department for advice. The following should **NOT** be released:

- information containing personal data about a third party (including names);
- 'sensitive personal data' (see section 3 of the Policy);
- data which is confidential at the time of request (eg exam results);
- data which is substantial in volume, time consuming or difficult to retrieve;
- information you are in doubt about releasing for any other reason.

In these circumstances, refer the enquiry to the Data Protection Officer in the Legal Department.

If you are asked for access to personal data by a third party (someone other than the data subject):
Contact the Data Protection Officer in the Legal Department.

A3 RECORD-KEEPING

Staff have a duty to ensure that records are: accurate; up-to-date; fair; kept and disposed of safely, in accordance with this policy and guidelines and any current University or departmental document retention policy / guidance.

Both manual records and computerised or electronic records must comply with the above requirements.

Staff should be aware that (with the exception of certain specified items of information, such as confidential references), **all** information held in MMU records, including emails and handwritten notes, may be disclosed to an individual under a subject access request (SAR) under the Act. It is essential that written statements about individuals are fair, accurate and factual and do not include personal comments.

A4 SECURITY

Staff responsibilities in relation to data security and confidentiality are outlined in section 4.1 of the Policy. All staff should be aware that they are responsible for the security of personal data.

Practical recommendations for keeping personal data safe and secure, include keeping the data, as far as possible:

- in a locked filing cabinet or drawer;
- password protected (if computerised);
- on disk which itself is kept securely.

It is recognised that it is impractical for information to be locked away at all times during the working day. Normal practice would be for filing cabinets and drawers to be unlocked during the day and locked overnight; however, staff must ensure that information is not accessible during the day to anyone who should not be permitted to see it.

When personal data is to be destroyed, paper or microfilm records should be disposed of by shredding or incineration; computer hard disks or floppy disks should be re-formatted, over-written or degaussed.

Staff should ensure that current University and/or departmental guidance regarding data retention periods are complied with. Standard recommended retention periods for student data are either 6 years from the date the student leaves the University (in accordance with the statutory limitation period for actions for breach of contract) or 3 months from a completion of procedures letter, based on the usual time limit for making a complaint to the Office of the Independent Adjudicator for Higher Education.

A5 PHOTOGRAPHS AND VIDEOS

A5.1 Display of Photographs

Photographs of staff and students may be displayed in University offices, corridors or teaching rooms. Anyone who objects to their photograph being displayed on University premises must notify their Head of Department, stating their reasons, in writing.

A5.2 Taking Photographs / Videos

Taking photographs or video recordings of individuals and small or organised groups (of staff/students/others) requires consent from the data subject. The data subject must be notified of the purpose of the photograph or video, prior to it being taken. Photographs and videos must not be used for a purpose to which the individual has not consented; any use or re-use for alternative purposes requires further consent from the data subject.

General photographs and video recordings of campuses or public places do not require consent or any specific action. The fact that someone is in a particular place at the time the photograph is accepted as a fact of life.

When taking photographs or videos of individuals or organised groups, the instructions below should be followed:

Individuals:

- before the photograph is taken, inform the data subject of the purpose for which the photograph will be used and any other necessary information, eg, whether it will be passed to a third party, displayed on the internet or used for marketing purposes;
- obtain the data subject's consent, using the Photograph Consent Form [attached], clearly advising them how to 'opt out' of any intended purpose;
- if 'natural' (non-posed) photographs/video footage (without the awareness of the data subjects) is required, inform the data subjects of the purpose and request consent as soon as it is taken. If consent is not given, the photograph must be destroyed immediately and its destruction documented.
- The Photograph Consent Form should be retained with the photograph.

Organised Groups (adults):

- inform the group of the purpose for which the photograph(s) are to be used;
- allow anyone who wishes to opt out to leave the group;
- note the date of each photograph and identity of the group (eg BA Human Communication, Year 2) to be retained with the original photograph.

Organised Groups (children): (under the age of 18)

- notify the school/college, or the parent/guardian of each child, of the purpose for which the photograph will be used;
- explain how data subjects may opt-out, and request consent from each parent/guardian. (In most instances, the school/college will prefer to contact or inform the parents and children);
- obtain written confirmation that the parents and children have been informed from the school/college, prior to taking the photograph(s);
- complete and sign the Photograph Consent Form – Schools [attached] and retain this with the relevant photograph(s).

A6 THE INTERNET

A6.1 Staff/Student Personal Data on the University's Website

Personal data may be available on the University's website and via the internet and will be available in countries which do not have a data privacy regime considered adequate by the EU. Such data may be made available as part of the normal organisational functioning and management of the institution. However, staff and students have the right to object (see section 5.3 of the Policy) to the use of their data where it would cause them significant damage or distress.

The use of personal data on the web for other purposes, such as publicity photographs, requires the consent of the staff and/or student(s) concerned.

A6.2 Collecting Personal Data

Web pages may be used to collect personal data, such as names and addresses of individuals requesting prospectuses, or registering to attend an open day. The web page/form should indicate the purpose for which the data is collected, the recipients to whom it may be disclosed and for how long it will be kept (eg "while we process your application", rather than a specific date).

Individuals must be given the opportunity to opt out of parts of the collection or any use of the data not directly relevant to the original purpose. For example, for individuals ordering prospectuses, if a follow-up scheme is used to discover why candidates did not come to the University, the individual should be notified of the scheme and be able to opt out of it.

THE MANCHESTER METROPOLITAN UNIVERSITY
LEGAL DEPARTMENT

PHOTOGRAPH CONSENT FORM

I consent to the use of photographs of **myself / my child** (*delete as applicable), taken by members of the University or by agents authorised on behalf of the University.

I understand that the photographs will be used for the following purposes(s):

……

……

……

I further consent to the use of the photograph(s) in official University publications and in University publicity material, including but not limited to, the University's prospectuses, annual report/review, newsletter, course leaflets, advertisements, web-site and online photographic image bank. ***If you do <u>NOT</u> agree to this further consent, please tick box:** ☐

Name of person being photographed : ……...

Signature : ……
(parent/guardian must sign for children under 18 years)

Name of parent/guardian (if applicable): ……..……..

Address: ……..……

……

University department/course (if applicable): ……..…..

Date: ……...

<u>For office use only</u>

Campus:	Department:
Project Name:	Job Number:
Photographer:	Notes:

THE MANCHESTER METROPOLITAN UNIVERSITY
LEGAL DEPARTMENT

PHOTOGRAPH CONSENT FORM – SCHOOLS

FOR COMPLETION BY MMU:

I confirm that the attached photograph(s) of children under the age of 18 years were taken by members of the University (or by agents authorised on behalf of the University) AND that **prior to taking the photograph(s)**:

		Tick to confirm
1.	I informed the relevant school/college that the photograph(s) will be used for the following purpose(s) [please specify]:	
2.	The school/college has confirmed in writing that it has obtained parental consent for each child featured in the photograph(s) and a copy of the written confirmation from the school/college is attached.	
3.	The school/college has confirmed verbally to me that it has obtained parental consent for each child featured in the photograph(s) AND I informed each child who I was and the purpose(s) for which the photograph(s) were being taken.	
4.	The parent/guardian of each child featured in the photograph(s) provided additional consent for the University to use the photograph(s) in official University publications and University publicity material, including but not limited to prospectuses, annual report/review, newsletter, course leaflets, advertisements, web-site and online photographic image bank.	

Name (of MMU member of staff): ……..

Signature: ……. Date: ……..

Faculty/Department: ……

Name of School / College …… Class: …….

For office use only

Campus:	Department:
Project Name:	Job Number:
Photographer:	Notes:

APPENDIX B – USE OF PERSONAL DATA IN RESEARCH

B1 USE OF PERSONAL DATA IN RESEARCH

Personal data used for research purposes (including research undertaken as part of an undergraduate dissertation), is subject to the Act and it is therefore essential to abide by this policy and guidance.

The checklist for processing personal data (see guidance section A2) should be followed, together with the guidance below:

- The data subject must be informed why the data is being collected and the purposes for which it will be used.
- Consent of the data subject must be obtained for both participation in the research project and the processing of data. Explicit (written) consent must be obtained for the use of sensitive personal data for the purpose indicated.
- Assurances should be given regarding the security of the data provided.
- It should **not** be possible to identify the data subject from the published results. The publication of unanonymised results requires the explicit written consent of the data subject.

Providing the checklist in the Guidelines for Staff and the above guidance is followed, the requirements of the Data Protection Act will be met.

B2 EXEMPTIONS

The Act gives **exemptions for research** (including statistical or historical purposes), where the data is not used to support measures or decisions relating to individuals, and its use is unlikely to cause substantial damage and/or distress to the data subject. Providing these conditions are met, it is permitted to:

- process the data for purposes other than those for which they were originally obtained (exemption from second principle). This means that data collected by the University for administrative purposes or for an earlier research project can be re-used for alternative (research) purposes without obtaining further consent from the data subject(s);
- hold the data indefinitely (exemption from fifth principle)

Furthermore, the data subject does not have a right of access to the data, providing it is processed for research purposes and the results do not identify the data subjects (exemption from section 7 of the Act).

APPENDIX C – DEALING WITH STUDENTS' PERSONAL DATA

This section is a brief summary of the main points covered in the Guidance. It indicates what staff must do to comply with the Data Protection Act and provides lists of personal data which may be disclosed, or are exempt from disclosure, to the data subject.

C1 IF YOU COLLECT, HOLD OR PROCESS STUDENT RECORDS:

- Read the Policy and Guidance in full.
- Follow the checklist in section A2 of the Guidance.
- Ensure the data is stored securely and is not disclosed unlawfully.
- Ensure that University and departmental policy and guidance regarding data retention periods is followed.

C2 PERSONAL DATA

The definition of personal data is described in section 3 of the Policy. It includes expressions of opinion about students and indications of the University's intentions in respect of students. It includes data processed electronically (via computer, web/internet) and information recorded manually as part of a filing system.

The Act is based on the premise of transparency. All personal data held may be disclosed to a data subject (in response to a request for access), although there are some exemptions under the Act.

C3 PERSONAL DATA WHICH MAY BE DISCLOSED TO THE DATA SUBJECT ONLY includes (but may not be limited to):

- Personal details including name, address, date of birth etc
- UCAS and University application forms
- Enrolment forms
- Academic or employment references received about an individual
- Class attendance records
- Health and medical matters
- Political, racial, religious or trade union information
- Any statements of opinion about abilities or performance
- Notes of personal supervision, including behaviour and discipline
- Disciplinary records
- Comments by tutors on coursework
- Comments of examiners on examination scripts
- Assessment/examination marks
- Examination Board minutes that refer to the individual
- Letters, e-mails, fax messages, internal memoranda, handwritten notes about students between staff/students, staff/staff, or staff/external parties.
- Correspondence relating to requests for review of decisions of Boards of Examiners

C4 DATA EXEMPT FROM DISCLOSURE TO THE DATA SUBJECT includes (but may not be limited to):

- References written by MMU staff about students (see section C6 below).
- Examination scripts (see section C5 below).
- Information subject to legal professional privilege.
- Correspondence where a third party might suffer damage or distress as a result of the disclosure. In some instances the removal of the name of the third party from an item of correspondence might be sufficient for information to be disclosed.

C5 EXAMINATIONS

C5.1 Examination results

Students are entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide.

Examination pass lists and degree classifications may be published on noticeboards within the University and in awards ceremony programmes. Students who do not wish their results to be published in this way, must notify the Director of Student Services & Deputy Registrar stating their reasons in writing, no later than seven days before their last examination or assessment. Publication may be withheld if it would otherwise be likely to cause unwarranted substantial damage or distress.

Examination results may not be divulged to students on the telephone unless, exceptionally, there is prior agreement to do so. Results may only be divulged by the Head of Department or Course Leader; and only to the student to whom they relate, providing that the student's identity is verified. This may be carried out by asking the student to confirm their registration number and date of birth or other personal information.

C5.2 Examination Scripts

The University is not obliged to disclose examination scripts to data subjects; however, internal and external examiners' comments written on the scripts **are** disclosable under the Act; and must be provided in legible form. "Examination" includes written assessment work and fieldwork, etc.

C5.3 Examination Board Minutes

Students have the right to request a copy of any examination board minute or report which refers to them, unless the data cannot be provided without disclosing information about other individuals.

C6 CONFIDENTIAL REFERENCES

Confidential references written by external referees **received by** the University may be disclosed to a data subject on request, however, it is for the University to decide whether or not to disclose a reference. Decisions will be made on a case by case basis with reference to the circumstances, the Act and current guidance from the ICO. Requests for references should be referred to the Legal Department. References disclosed may be anonymised.

Confidential references **written by** a member of University staff about a student or member of staff and sent to an external individual or body are not disclosable by the University. (Note that the data subject may ask for a copy of the reference from the party who receives the reference).

C7 TRANSCRIPTS

Transcripts are official University documents verifying a student's awards or marks. The Act provides rights in relation to the information held and processed by the University, but not in respect of how the University formats or presents that information when it is released. Student transcripts are generally dealt with by the Faculties. For further information see the Awards & Conferments section of the website. The University may withhold the official transcripts of debtors.