Procedures on confidentiality and sharing of student Information

University Statement on Confidentiality

Aberystwyth University (AU) will respect the confidentiality of information provided to us by students and staff in line with the Data Protection Act 1998 and its own information-sharing protocols. Confidential information will only be shared where express permission has been given or where information sharing is necessary by reason of safety or legality.

Scope

This document applies to all personal information relating to students held by AU, irrespective of ownership. Personal information is defined for the purposes of these procedures as being any information that can identify an individual.

The document applies to all contractors and agencies operating on behalf of the University. For the purposes of these procedures the term “employee” covers all of these groups.

These procedures outline AU’s approach to ensuring all employees effectively process and manage students' personal information within set standards, to protect the privacy and confidentiality of individuals, and to comply with the principles and requirements of the Data Protection Act 1998 and other legislation. The procedures set out how student information will be managed and how confidentiality will be protected by the University.

The procedures should be read in conjunction with the Aberystwyth University Data Protection Policy: https://www.aber.ac.uk/en/infocompliance/policies/dp/

Purpose

The purpose of these procedures is:

- To promote the effective, consistent and legal, processing of personal information
- To ensure that all employees and students in contact with AU are aware of their responsibilities in relation to the processing of students' personal information and to the law surrounding its use.
- To ensure all employees and students of AU are aware of the consequences of the misuse or abuse of personal information.
- To ensure compliance with legislation, guidance and standards relating to the processing of personal information and its confidentiality.

1. What is Confidential Information?

1.1 Confidential information is any information to which the common law “duty of confidence” applies. A duty of confidence is created when “private” information has

been passed on in such a way that the person receiving it was aware, or should have been aware, that the information was being provided on the basis of confidentiality. The legal test is whether a "reasonable" person would think the recipient ought to have known that the imparted information was confidential.

1.2 Information of a personal nature (that which identifies an individual), or sensitive personal information, as defined by the Data Protection Act (that which relates to personal characteristics such as racial origin, religious belief and sexual orientation) may be examples of confidential information.

2. Promises of Confidentiality

2.1 Absolute promises of confidentiality must never be made.

2.2 Decisions as to whether information needs to be shared can only be made when the staff member is in full possession of the facts and therefore no "up-front" guarantees concerning confidentiality can ever be made. Staff members are able to state that the confidentiality of the student will be respected in sharing the information with as few individuals as possible.

3. Consent to Share Information

3.1 The University understands confidentiality to mean that NO information regarding a student shall be shared either directly or indirectly with any other department of the University, or any external agency or person, without that student's prior, express consent, subject to exceptions relating to safety and legality. [See sections 6, 7 and 12]

3.2 This does not apply to information declared on UCAS application forms or anonymised details which may be used for statistical and planning purposes.

3.3 It is the responsibility of the individual staff member to ensure that they obtain consent before sharing any information or taking any action on behalf of a student. Students are able to specify which individuals/teams/departments they are willing for information to be disclosed to.

3.4 Written consent is preferable wherever possible. Verbal consent will suffice if explicit written consent is not possible, but written consent should be sought as soon as possible after the sharing of information has occurred.

4. Where consent is refused

4.1 A student's decision to not give consent for the sharing of information should be respected unless there are concerns of safety and / or legality.

4.2 Potential consequences of not sharing information should, however, be discussed with the student, particularly where it could limit their access to support. A decision of this kind should be documented.

5. Parents and Emergency Contacts

5.1 Aberystwyth University acknowledges that students are autonomous adults and so will not discuss any details of a student with their parents or other family member unless prior express permission has been obtained from the student.

6. Circumstances where Confidential Information Must Be Shared Without Consent

6.1 Confidential information must not be shared without consent unless:

- An organisation requesting the information has a legal right to the information (e.g. the police investigating a crime. Please see https://www.aber.ac.uk/en/media/departmental/studentsupport/responding-to-police-requests-final-version.docx for further information).
- To comply with a court order, including the coroner's court.

Requests from the police and courts will generally be in writing

- It is a requirement of law. This includes, but is not limited to, laws relating to drug trafficking, terrorism, money laundering and safeguarding. (Please see the Aberystwyth University Safeguarding Policy for further details: http://www.aber.ac.uk/en/hr/policy-and-procedure/safeguarding/)
- It is believed to be in the best interests of the student. This particularly relates to circumstances where there is a perceived immediate and serious threat to the health and safety of the student concerned or to others.
- It is believed to be in the overall public interest and in any particular instance the public interest is judged to outweigh other considerations.
- Where an individual's professional fitness to practice may be compromised. Fitness to practice concerns should be tested with reference to documented criteria from the appropriate professional body.

6.2 Please ensure that you consult with the Data Protection Manager before sharing in any of the above scenarios (mailto:infocompliance@aber.ac.uk).

7. Circumstances where Confidential Information May Be Shared Without Consent

7.1 Consent to share information should be sought wherever practicable BUT the student should NOT be informed if it is likely to increase the perceived level of risk to the student or to a third party.

7.2 Breaching confidentiality should be a joint decision with the student wherever possible, but if this is not possible, then consultation with a more senior colleague or an individual from a professional service such as the Student Wellbeing Service is recommended and appropriate.

7.3 However, where there are clear indications that the student is in imminent and serious danger the emergency services should be contacted as quickly as possible.

8. Disclosure of a Disability

8.1 The University aims to provide an environment in which students feel comfortable about disclosing a disability. For students there are advantages in disclosing a disability, for example:

- to receive appropriate learning and accommodation support or adjustments;
- to receive information on potential sources of funding to pay for student-related disability requirements or
- to receive information about the range of services to which they may be entitled.

8.2 Students can disclose a disability at any time and to anyone. This may be either formally or informally. However, students should always be encouraged to disclose formally because of the potential benefits as outlined above. http://www.aber.ac.uk/en/student-support/accessibility-advice-and-support/

8.3 Students who do not formally disclose their disability may not be fully aware of, nor receive, the full range of support or adjustments to which they may be entitled. This could impact on their academic progress.

8.4 The student disclosing a disability should be encouraged to make contact with the appropriate Departmental Disability Coordinator, who will then communicate with the student regarding next steps. If the student prefers, a staff member may do this on the student's behalf but should only inform the Departmental Disability Coordinator with the student's consent.

8.5 If the student chooses not to make a formal disclosure they should be advised that this may prevent or restrict the support the University can offer.

8.6 If a staff member is notifying the Departmental Disability Coordinator directly, the student's name and contact details and a brief description of the nature of the disclosure will be sufficient. Detailed sensitive information should not be included.

9. Record Keeping

9.1 Any contact (including meetings and conversations) involving the disclosure of potentially sensitive or confidential information should be recorded.

9.2 Records must only contain factual information, and should not include any comments or judgements on areas outside of the individual staff member's professional competence. All records must be kept securely in an appropriate location. This may be in the departmental student file, on SharePoint, in a file on a shared drive or other system on the University network.

9.3 Access must be restricted only to those who have a need to know.

9.4 Wherever possible, the data subject (the student) should be made aware that such records will be created and retained.

10. Processing Personal and Confidential Information

10.1 'Processing' of personal information encompasses everything that we do with personal information including the reading, sharing, transferral or disclosure to another organisation or internally.

10.2 Personal information must be processed in accordance with the eight principles under the Data Protection Act 1998 unless an exemption applies. http://www.aber.ac.uk/en/infocompliance/dp/

10.3 Employees must respect personal information to which they have access to and treat it in the manner in which they would expect their own personal information to be treated.

10.4 Employees must have regard and respect for the privacy of colleagues and students, and process personal information accordingly.

10.5 10.5 No employee has an automatic right to access any or all personal information held by the University by virtue of their position or the fact that they are employed by the organisation. Access to personal information must be accepted by all to be on a need-to-know basis only.

10.6 Personal information should be deleted and disposed of as appropriate. Details relating to the retention of documents are available from the University's Records Manager: https://www.aber.ac.uk/en/infocompliance/rm/

10.7 Personal information should be held securely, and accessible only to those with a need to know. Managers are responsible for ensuring that personal information is protected by appropriate security (i.e. relevant to the sensitivity of the personal information).

10.8 Personal information must not be transmitted electronically outside the University without appropriate security or encryption.

10.9 Use of an AU email account is mandatory when communicating about University business.

10.10 Care must be taken when processing personal information via email, in particular that limited levels of detail are used, and that dissemination is restricted to those with a need to know.

10.11 When information is collected or disclosed the student will be informed, as far as is practicable, of the purposes for which the information will be processed, and will be provided with any other relevant details regarded the processing.

10.12 Complaints regarding the management or processing of personal information by Aberystwyth University should be referred to the Information Compliance Team (mailto:infocompliance@aber.ac.uk).

11. Inappropriate and Unacceptable Behaviour in respect of Personal Information

11.1 Unacceptable behaviour includes:

- Unauthorised accessing of personal information
- Unauthorised disclosure of personal information
- Unauthorised access and disclosure of information includes conducting confidential conversations in public areas such as corridors, staff rooms and other inappropriate environments
- Sharing information too widely (for example cc'ing across a department) or including inappropriate levels of detail
- Use of non-University email addresses
- Unauthorised use of personal information (e.g. not for reason given to the data subject)
- Non-adherence to Aberystwyth University's information-sharing protocols

11.2 Student information must not be used for:

- Any illegal purpose.
- Any purpose which is inappropriate by virtue of the fact it may cause embarrassment or distress to another person or may bring Aberystwyth University into disrepute.

  This is not an exhaustive list and should not be considered so.

11.3 Employees are required to notify their Line Manager and the AU Information Compliance Team (mailto:infocompliance@aber.ac.uk) if they become aware, or suspect, that personal information relating to either employees or students is being misused or handled inappropriately.

12. Legislation

The following legislation should be considered when using and sharing personal data:

12.1 **The Caldicott Report** (1997, Revised 2013)
https://www.gov.uk/government/publications/the-information-governance-review

Whilst the Caldicott Report is used primarily to inform services within the NHS, its six key principles may be considered good practice in relation to personal information and the protection of confidentiality.

1. Justify the purpose

   Every proposed use or transfer of personal identifiable information within or from an organisation should be clearly defined and continuing uses should be reviewed.

2. Don't use personal identifiable information unless absolutely necessary

   Personal identifiable information shall not be used unless there is no alternative.

3. Use the minimum necessary personal identifiable information

   Where use of personal identifiable information is considered to be essential, each individual piece of personal information used must be justified.

4. Access to personal identifiable information should be on a strict need to know basis

   Only those individuals who need access to personal identifiable information and confidential material should have access to it, and they should have access only to items of personal information that they need to.

5. Everyone should be aware of their responsibilities

   Actions should be taken to ensure that all staff who handle personal identifiable and confidential information are aware of their responsibilities and obligations to respect confidentiality.

6. Understand and comply with the law

   Every use of personal identifiable information must be lawful.

12.2 Data Protection Act (1998) http://www.legislation.gov.uk/ukpga/1998/29/contents

The purpose of the Act is to prevent personal information being used for purposes other than that for which it has been collected and states that data should be:

- Obtained and processed fairly and lawfully.
- Obtained for one or more specified purposes.
- Accurate and where possible kept up to date.
- Kept for no longer than is necessary.
- Processed in accordance with the rights of the data subject.
- Stored using appropriate measures against accidental loss or destruction or damage to personal data.
- Data should not be transferred to a country outside of the European Economic Area (EEA) unless that country ensures an adequate level of protection for the rights and freedoms of data subjects.

The Act refers to "personal data" which means data that relates to an identifiable individual, and "sensitive personal data" which relates to data that includes, but is not limited to, the data subject's racial origin, political or religious belief, trade union membership, physical and / or mental health condition, sexual life, or information relating to an offence.

13. Non-Compliance with legislation and policy

13.1 All employees and students must be aware of their obligations with regard to the disclosure and the processing of personal and confidential material.

13.2 Non-compliance will be dealt with under AU's Disciplinary Procedures and may be considered an act of gross misconduct.

14. Implementation and Review

14.1 These procedures will be available via the AU webpages and will be reviewed at least annually and more frequently where needed.

Version:	2.0	Publication Date:	24.2.16
Reason for update:	Review and update of information		
Approved:	Student Support Committee 24.2.16	Effective From:	24.2.16
Other Stakeholders	AQRO, Information Compliance, Information Services		
Contact:	Caryl Davies, Director of Student Support Services ccd@aber.ac.uk		