6.4.2 Personal Data Usage and Public Information Policy

1. Purpose

ADA University collects, stores and processes data to improve the quality of its academic offerings, to facilitate decision-making processes, and to provide relevant information to the public and other relevant parties. In this context, it is essential to ensure that data is handled in an ethical manner and according to applicable legal regulations. The objective of this policy is to delineate the requirements for the collection and storage as well as the processing and usage of data for non-research purposes at ADA University.

2. Scope and Recommendations

This document covers the collection, storage, processing and usage of personal data for non-research purposes in all areas covered by ADA University's *Academic Quality Assurance Standards and Guidelines*, namely the academic program (including teaching, learning and assessment), research, students (including graduates), faculty and staff. It particularly refers to the rapidly developing field of learning analytics whenever appropriate.

All members of ADA University that are dealing with personal data and/or have partial or full access to its *Academic Performance and Quality Assurance Database* and/or its physical archive are expected to be thoroughly familiar with this policy and to strictly adhere to its requirements and procedures.

This policy should be read in conjunction with ADA University's *Data Management and Reporting Regulations*.

3. Definitions

In accordance with the *Law of the Republic of Azerbaijan On Personal Data* and the European *General Data Protection Regulation (GDPR)*, *Data* in this policy is defined as "personal data". *Personal Data* refers to any information that allows, either directly or indirectly, to identify a natural person.

The *General Data Protection Regulation (GDPR)* is a European regulation on the protection of personal data throughout the European Union.

A *Data Subject* is an identified or identifiable natural person whose data is gathered and used. The term *Subject* connotes both that the person is *subject to* the processes of data collection and usage *and* that it must (for ethical and legal reasons) be considered as an *active subject* in these processes.

Data Pseudonymization requires that personal data is processed in such a manner that it cannot be attributed to a data subject without additional information. Data subjects can still be re-identified by the use of such additional information.

Data Anonymization describes a process in which personal data is permanently stripped of all information that may lead to the identification of a data subject.

The *Academic Performance and Quality Assurance Database* serves to collect, organize and keep all the quantitative and qualitative information (raw data) required to assess the University's performance in all the areas relevant to the evaluation and improvement of academic quality.

Learning Analytics describes the collection, analysis and usage of data on students and their learning activities with the objective of understanding and improving educational processes and providing effective support to learners. Learning analytics poses new challenges to the ethical and legal usage of data due to the considerably extended scope and amount of data that may be systematically generated and gathered by digital information systems.

4. Data Usage and Protection

4.1 Purposes of Data Gathering and Usage

a. The collection and usage of data benefits both the institution and its individual members.

b. Data serves to evaluate the University's performance in all areas relevant to academic quality. These areas include the academic program; teaching, learning and assessment; research; students (including graduates); faculty and staff. The analysis of data allows for well-informed decisions and for the improvement of the institution's performance in these areas.

c. Data serves to support students in their learning activities and progress. Learning analytics and the analysis of data enable the University to provide feedback to students and to identify areas in which they may (individually or collectively) be in need of additional learning opportunities in order to be more successful in their performance.

d. Data serves to support faculty in their teaching and research activities. The analysis of data enables the University to provide feedback to its faculty members and to identify areas in which they may (individually or collectively) need to improve and/or may require additional support and training opportunities in order to be more successful in their teaching and research.

e. Data serves to facilitate internal administrative processes. It is used (for example) to organize events and certificate programs, to ensure a well-structured process of personnel recruitment, and to efficiently communicate throughout the University.

f. Data is used for the information of relevant stakeholders and thus for the purposes of reporting, accountability and transparency (for details, see chapter 5.1 below).

4.2 Legal and Ethical Issues

a. *Infringement on Privacy*: In general, the collection and usage of data could infringe upon the privacy of a data subject, which is considered to be a fundamental human right. It could infringe upon the informational self-determination of that subject, which describes the right to decide which information should or should not be disclosed to others.

b. *Re-Identification*: More specifically, the collection and usage of data could result in the re-identification of a data subject by using multiple datasets and by aggregating de-identified data. This in particular would violate the right of informational self-determination and allow discrimination against individual members of the University.

c. *Lack of Transparency*: Data could be collected and used for purposes other than those communicated to data subjects. This would further infringe upon the right of informational self-determination and prevent any intervention on the part of data subjects.

d. *Excessiveness of Data*: The amount of data gathered could exceed the scope of what is needed to fulfill well-founded, clearly defined and explicitly communicated purposes. This would result in a further encroachment on the privacy and rights of the data subject.
e. *Inadequacy of Data*: The data collected and used could be incorrect. It could misrepresent a data subject and/or his/her academic performance and thus unfairly advantage or disadvantage certain members of the University.
f. *Unauthorized Access*: Members and/or non-members of the University could gain unauthorized access to (and use) data stored on the *Academic Performance and Quality Assurance Database* and/or in the University's physical archive. This would represent a breach of confidentiality and infringe upon the individual's right of informational self-determination.
g. *Reduction*: Learning analytics and the focus on data carry the risk of reducing students to a certain set of quantitative and/or qualitative information. Yet, data gathered by the University can only provide an incomplete picture of individual students, whose needs and performance are also influenced by factors that are not covered by the University's *Academic Performance and Quality Assurance Database*.
h. *Generalization*: The use of aggregate data could have adverse effects on individuals. It could result in simplification and disregard the specific needs of individual members of the University.
i. *Reinforcement of Bias*: The collection and usage of data could impede the positive development of students and other members of the University. It could result in oversimplified categorization and thus in the perpetuation of ethnic and/or sociocultural stereotypes and in unintended discrimination.
j. *Closure*: Data could be interpreted in a way that projects the prior academic performance of data subjects into the future. This would restrict individual opportunities for development and interfere with both the fundamental openness of the future and the principle of equity.

4.3 Requirements and Procedures for Data Usage and Protection

a. The following requirements and procedures must ensure that data is used in both a legal and ethical manner (addressing all the issues mentioned above in chapter 4.2) while, at the same time, enabling an efficient use of data (for details, see the University's *Data Management and Reporting Regulations*) for the purpose of internal quality assurance and for the fulfillment of all obligations to accrediting agencies, the Ministry of Science and Education and the Azerbaijan National Academy of Science, and the general public (for details, see chapter 5 below).
b. The following requirements and procedures thus apply both to the internal usage (data gathering, storing and processing) and the external usage of data (disclosure of information to accrediting agencies, the Ministry of Science and Education, the Azerbaijan National Academy of Science, and the general public).
c. Data may be disclosed to third parties other than those defined in 4.3.b for well-founded academic and/or administrative purposes and/or if the disclosure of data is legally required. Any such disclosure must strictly follow the requirements and procedures outlined in this document. All third parties that are no state entities must sign a *Non-Disclosure Agreement* with ADA University before any data may be provided to the respective party.
d. The following requirements and procedures are based on the *Law of the Republic of Azerbaijan On Personal Data*, on the European *General Data Protection Regulation (GDPR)*, and on international best practices.
e. *Data Privacy*: Personal data must be protected against unauthorized access, usage, change, or destruction. This includes protection against the unwarranted disclosure of information to internal and/or external stakeholders and against the re-identification of data subjects from aggregate data or from the combination of several datasets by anyone other than those University member(s) having access to the respective datasets. It requires the unambiguous

identification of those members of the University that have (partial or full) access to the University' *Academic Performance and Quality Assurance Database* and/or its physical archive as well as the precise classification of data according to data privacy categories. Information exempted from the requirement of privacy is data that is made public by individual members of the University as part of the academic process (such as information on publications). Further details on access to the University's database and on data classification can be found in chapter 4.4 below.

f. *Data Pseudonymization*: Data privacy requires that personal data used for reporting and information purposes be processed in a manner that it cannot be attributed to a specific data subject. This includes the de-identification and aggregation of data.

g. *Data Protection*: Data privacy requires appropriate technical and physical solutions to safeguard (protect) data. Members of the University involved in data management and data reporting (Data Operators) may only use software applications that have been approved by the University for these purposes. This includes all those members of the University that receive data and reports in a digital format (Data Users). The Office of IT and Information Services is responsible to provide a current list of software approved by the University. Learning analytics at the University is conducted using *Blackboard Analytics for Learn*. Any other software used for this purpose requires the prior approval of the Office of Faculty Affairs and Academic Administration and the Office of IT and Information Services. To the extent possible, the latter Office must also prevent any breaches of the integrity of the University's *Academic Performance and Quality Assurance Database* by applying the tools and techniques available at the University. Paper-based data must be stored safely by those gathering and processing the respective data. It must be moved to designated archives at regular intervals.

h. *Purpose Limitation*: The University must ensure that data is gathered, stored and processed only for legitimate and clearly specified purposes. These purposes must be explicitly and comprehensibly communicated to each data subject whose data is gathered, stored and processed by the University or any of its members. It is the shared responsibility of the University's Data Protection Officer and the Office of Quality Assurance and Accreditation to precisely determine, regularly assess and potentially reevaluate the purpose(s) of each dataset stored and used by the University (for details on the Data Protection Officer, see chapter 4.4 below). To fulfill this responsibility, they will cooperate with relevant administrative and/or academic units of the University whenever necessary.

i. *Data Minimization*: The University must ensure that it limits the collection of personal data to what is required to fulfill specific and clearly defined purposes. It must thus ensure that it gathers, stores and processes as much data as necessary and as little data as possible. This applies, in particular, to data gathered and processed for the purposes of learning analytics, which has the potential to significantly extend the limits of information gathered on individual students. It is the shared responsibility of the University's Data Protection Officer and the Office of Quality Assurance and Accreditation to regularly assess and potentially reevaluate the significance of all data gathered, stored and processed by the University. To fulfill this responsibility, they will cooperate with relevant administrative and/or academic units of the University whenever necessary.

j. *Data Accuracy*: All data stored and processed by the University must be valid and reliable. Data accuracy is the responsibility of all administrative and academic members and units of the University (also see chapter 4.1 of the University's *Data Management and Reporting Regulations*).

k. *Positive Intervention*: Data is expected to serve the major purpose of improving academic processes and the performance of the University's individual members. This implies that adverse effects should be minimized or altogether avoided. Such effects may result from (for example) generalization or simplification when analyzing and using data.

l. *Equitable and Conscious Data Usage*: Positive intervention presupposes that data is used consciously by all members of the University and in a manner that prevents any form of reduction, generalization, reinforcement of bias and/or closure. This requires that all those dealing with personal data are regularly and thoroughly trained in the adequate use of such data (as outlined below).

m. *Information and Consent*: The University gathers and uses a variety of personal data (for details, see the University's *Data Management and Reporting Regulations*) to comply with legal requirements and to be able to fulfill its institutional purposes (for details, see the University's *Statement of Institutional Purposes*). In this context, the University must provide comprehensive and comprehensible information to those whose data is gathered and used about (1) the kind of data that is collected, (2) the purposes that it is used for, (3) the ways in which it will be stored and processed, (4) the ways in which it will be protected, (5) the period for which it will be stored, (5) the benefits derived from data gathering and usage, (6) the members of the University operating the data, and (7) the rights of data subjects in relation to the storage and usage of their data. The University must acquire unambiguous consent that clearly indicates the respective data subject's informed agreement to the gathering and processing of his/her personal data. This consent must be acquired using the University's *Personal Data Consent Form*, which must clearly refer to the data that is gathered and used and the purpose(s) for which this is done. It must also detail the conditions for the refusal or withdrawal of consent, the periods for which data will be stored, and the University's procedures for data archiving and destruction. Informed consent is necessary for all data that the University is not mandatorily required to collect and process in order to comply with the legal regulations of the Republic of Azerbaijan. It is explicitly required for all data gathered and processed for the purposes of learning analytics. It must be renewed if data is to be used for purposes other than those for which initial consent was given. If a person refuses to give (or withdraws) his/her consent to provide relevant personal data that (1) the University is not legally required to collect, store and use, that (2) is lawfully collected, stored and used, and that (3) is necessary for the effective operation of the University (and for the fulfillment of its institutional purposes), this person must be made aware that this may result in the University not (or no longer) being able to provide education, employment and/or other services.

n. *Accessibility and Intervention*: At regular (and reasonable) intervals, and to the extent that this can reasonably be accomplished, all members of the University have the right to access their personal data that is collected and stored by the University and to receive a digital copy of this data as well as detailed information on its usage. They may thus verify data and/or request that personal data be rectified (in case data should be incorrect) and/or deleted. They may also ascertain that their data is used in a lawful manner and request that the use of their data be restricted. Deleting data and/or restricting its usage is not permissible in cases where this would violate any legal regulation(s) of the Republic of Azerbaijan and/or the University's obligation to document academic processes and/or their outcomes. Neither is it permissible in cases of an overriding public interest that requires the disclosure of information on the University. If a person requests that data be deleted and/or its lawful usage be restricted which (1) the University is not legally required to collect, store and use, which (2) is lawfully collected, stored and used, and which (3) is necessary for the effective operation of the University and for the fulfillment of its institutional purposes, this person must be made aware that this may result in the University no longer being able to provide education, employment and/or other services.

o. *Complaint Resolution*: Individual members of the University may address the Data Protection Officer if they suspect a violation of the requirements for data usage and protection outlined in this document in general and/or their right of informational self-determination in particular. The Officer will investigate every suspected violation reported and (if verified) initiate a resolution process as outlined below in chapter 4.5. All complaints must be treated with strict confidentiality. They are to be shared only with those actors mentioned in chapter 4.5 below that are involved in the process of complaint resolution. If the latter requires that the name(s) of the complainant(s) be disclosed to those accused of a violation of data privacy, usage and protection requirements, prior consent of the complainant(s) needs to be obtained. The interests of the latter are to be protected at all times, and the Data Protection Officer must ensure that they will not experience negative consequences (retaliation) as a result of their complaint.

p. *Data Storage Limitation*: The University must ensure that data is stored for no longer than is strictly necessary to fulfill the purposes for which the data was gathered and processed. For each dataset, and in accordance with international best practices and with the minimum legal retention requirements stated in the *Law of the Republic of Azerbaijan On Personal Data*, the University's Data Protection Officer and the Office of Quality Assurance and Accreditation shall define a maximum period for which the respective data may be stored. Data subjects have the right to request that their data be erased after the respective maximum period and/or whenever data is no longer required to fulfill the purpose(s) for which it was gathered and stored. This right particularly applies to data gathered and processed for the purposes of learning analytics, which is frequently of temporary significance to support the learning progress of individual students. Data exempted from the requirement of erasure is data that is of continuous public interest, that is legally required to be archived, and/or that is indispensable for the accountability and/or the further development and improvement of the University. Permanently archived personal data must (after the respective maximum storage period) be fully de-identified and be stripped of all personal information, provided that the purpose(s) for which the data continues to be stored can be fulfilled in that manner. In that case, data subjects have the right to request the anonymization of their personal data.

q. *Primacy of Privacy*: As a general rule, and in addition to the requirements and procedures outlined above, all those involved in the process of data collection and usage shall always consider the interests of the data subject and, in case of doubt, give preference to these interests.

r. *Data Literacy*: The University must ensure that all its members (administrators, faculty, students) are regularly trained in the appropriate use and protection of data. Students, in particular, are to be made aware of their right of informational self-determination. The organization and delivery of trainings and information sessions is the shared responsibility of the University's Data Protection Officer, the Office of Quality Assurance and Accreditation, and the Office of IT and Information Services.

4.4 Data Privacy and Data Classification

a. Data privacy requires that access to the University's *Academic Performance and Quality Assurance Database* and its physical archive is strictly limited.

   (1) Partial or full access to the database and/or the archive is only granted to those members of the University that are involved in the processes of data management and data reporting (also see chapter 4.2 of the University's *Data Management and Reporting Regulations*).

   (2) University members seeking (partial or full) access to the database and/or archive must submit a request to the Data Protection Officer, using the University's *Data Access Form*. Permission to (partially or fully) access the database and/or archive may only be given if required by the respective member of the University to fulfill his/her duties. Such permission needs to be confirmed by the Vice Rector for Institutional Effectiveness and Development before becoming effective.

b. Data privacy requires that the University has a Data Protection Officer.
   (1) The Data Protection Officer is responsible to monitor and ensure compliance with the data usage and protection requirements outlined in this document.
   (2) The Data Protection Officer represents the interests of data subjects and must investigate any suspected violation of these requirements reported to him/her by any member of the University. In case of a verified violation, the Data Protection Officer will initiate appropriate steps to protect the rights of the affected data subject(s) as outlined below in chapter 4.5.
   (3) The Data Protection Officer is elected by the Quality Assurance Committee and appointed by the Rector of ADA University for the duration of an entire quality review cycle (5 academic years). He/she may be reelected and reappointed once. The Data Protection Officer can only be removed from office (by a majority of the Committee's members) in case of a serious neglect of duty. The Committee's decision requires the approval of the Rector. The Data Protection Officer may appeal the decision by submitting a written complaint to the University Senate, who will make the final decision.
   (4) The Data Protection Officer annually reports to the Quality Assurance Committee.

c. Data privacy requires that the University has one or several specifically appointed Data Analyst(s).
   (1) Data Analysts are responsible for data reporting. They must ensure that data is processed safely at all times. They may only use software applications approved by the University. The University must ensure that they are specifically trained in the requirements of data privacy and protection.
   (2) Data Analysts are part of the Office of Quality Assurance and Accreditation. Data reporting may partly be delegated to members of other Offices (if required).
   (3) Data Analysts will regularly report to the Director of Quality Assurance and Accreditation and promptly submit any suspected violation of the University's data protection requirements to the Data Protection Officer.

d. Data privacy requires that all Data Operators and Data Users strictly adhere to the requirements for data usage and protection outlined in this document. Data Operators are all members of the University that collect, edit, organize, store, process and/or analyze personal data. Data Users are all members of the University that access personal data gathered and processed by the University. All Data Operators and Data Users must submit any complaint and/or suspected violation of the requirements for data usage and protection to the Data Protection Officer.

e. Data privacy requires that the Office of IT and Information Services provides technical support and guidance to all members of the University dealing with personal data whenever required. The Office is furthermore required to continually monitor the University's software infrastructure and to suggest potential improvements related to the University's *Academic Performance and Quality Assurance Database* in general or to the requirements and procedures for the usage and protection of personal data in particular whenever appropriate.

f. In order to ensure a high level of data privacy, personal data is classified into 3 categories.
   (1) Data classified as *public* is personal information that is generally made available to a wider audience as part of the academic process and/or that is of a general and overriding public interest. This includes information on issues such as research outcomes (faculty), degrees acquired (faculty), or rewards received (faculty, staff, students). Such personal data does not require the consent of the data subject to be made public by the University.
   (2) Data classified as *confidential* is personal information that is not generally made available to a larger audience and/or the public. This includes information on, for example, student performance, faculty evaluations, or graduate employment. Such personal data requires the explicit and informed consent of the data subject to be gathered and used. It must be processed in such a manner that it can no longer be attributed to a specific data subject.

(3) Data classified as *sensitive* is confidential personal information that, if made available to a larger audience, could have a significant negative impact on the data subject. This includes information on the ethnic and/or sociocultural background of the data subject. Such personal data must only be accessible to specifically designated members of the University. It must be kept separate from all other personal data and may only be used for restricted purposes (such as reporting to the Ministry of Science and Education). Personal data must be stripped of such information before being made accessible to other members of the University as defined above in chapter 4.4.a.

(4) It is the shared responsibility of the University's Data Protection Officer and the Office of Quality Assurance and Accreditation to determine, regularly assess and potentially reevaluate the classification of all data gathered and used by the University (information on the latter can be found in the University's *Data Management and Reporting Regulations*).

4.5 Breaches of Data Privacy and Unauthorized Data Usage

a. The University will investigate all instances in which a breach of data privacy and/or an unauthorized use of data may have occurred.

b. Each instance must be reported to the University's Data Protection Officer. In case of a verified breach of data privacy and/or misuse of data, the Officer will notify the data subject(s) affected by the occurrence (if applicable). In conjunction with the Office of Quality Assurance and Accreditation and the Vice Rector for Institutional Effectiveness and Development, he/she will furthermore undertake all steps required (1) to mitigate negative consequences for the respective University member(s), (2) to prevent further breaches and/or misuse of data, and (3) to potentially sanction those responsible for the occurrence according to the University's *Honor Code* and *Employee Handbook* as well as the legal regulations of the Republic of Azerbaijan. Sanctions are determined by the University's Honor Committee, who will come to a decision according to the procedures outlined in the 2 documents previously mentioned. Before undertaking any legal steps, the Data Protection Officer and the Honor Committee shall determine whether the occurrence can be solved by mediation.

c. The procedures outlined above also cover breaches of data privacy and/or the unauthorized use of data by non-members of the University.

d. Data breaches that involve gaps in and/or failures of the University's IT infrastructure must additionally be reported to the Office of IT and Information Services. In conjunction with the Data Protection Officer, the Office will undertake all steps required to prevent such breaches and suggest improvements to the IT security of the information systems and tools used by the University.

5. Transparency and Public Information

5.1 Purposes of the Disclosure of Information

a. As part of its reporting processes, information is made available to relevant members of the University. This contributes to the institution's self-transparency and allows for the internal assessment and enhancement of academic quality and for the further development of the institution.

b. Information is made available to national and international accrediting agencies. The reports submitted to these agencies further contribute to the institution's self-transparency and to the continuous improvement of the University's performance in key academic areas.

c. In accordance with the legal regulations of the Republic of Azerbaijan, information is made available to the Ministry of Science and Education and the Azerbaijan National Academy of

Science. The official reports submitted to the Ministry and the Academy provide a regular account of the University's activities and performance in key academic areas.

d. Information is made available to the general public, to current and prospective students, and to other interested groups. In the context of its institutional purpose of serving the needs of the community and society, the University thus ensures transparency by giving a regular account of its activities and performance.

5.2 Disclosure of Information

a. Information made available to internal and external stakeholders must be restricted to what is necessary to fulfill the purpose(s) envisaged by the disclosure of that information.

b. Information to internal and external stakeholders must be made available in accordance with the data classification outlined above in chapter 4.4.

c. Information made available to internal and external stakeholders must be meaningful. It must be accessible and comprehensible to the intended target audience.

d. Information is made available via reports, the University's website, its Academic Catalogue, and further printed and/or digital information material.

e. Internal reporting is based on the data usage and protection requirements outlined in this document. It covers all the areas included in the University's *Academic Quality Assurance Standards and Guidelines* in general and its *Data Management and Reporting Regulations* in particular. This includes (for example) data on student enrollment and retention, student performance and graduation, learning outcome implementation, exchange program participation, faculty performance and evaluation, research projects and output, and graduate employment. All personal data that is used in internal reports and that is not classified as *public* must be de-identified. Exceptions are only permissible in cases where the overriding purpose of quality assessment requires the identification of individual members of the University (as in the case of faculty evaluation). In such cases, the explicit and informed consent of the respective data subject(s) is required, and those bodies and members of the University involved in the process of quality assessment must treat personal data confidentially and in accordance with the data usage and protection requirements outlined in this document. Unless stated otherwise in the University's *Academic Quality Assurance Standards and Guidelines*, reporting is the responsibility of the Office of Quality Assurance and Accreditation.

f. Information reported to accrediting agencies is based on the legal regulations of the Republic of Azerbaijan (national agency) and on the requirements of the respective accrediting organization (international agencies). It thus covers all areas and data necessary to comply with the standards for accreditation of the respective agency, including (for example) information on degree programs and requirements, program effectiveness, student enrollment and retention, teaching and learning, student assessment, quality assurance, and the University's body of students, faculty and staff. Data submitted to the national Agency for Quality Assurance in Education will be identifiable or de-identified according to the applicable legal regulations of the Republic of Azerbaijan. In the case of international agencies, all personal data that is not classified as *public* must be de-identified prior to being submitted to the respective organization. The submission of information to national and international accrediting agencies is the responsibility of the Office of Quality Assurance and Accreditation.

g. Information reported to the Ministry of Science and Education and the Azerbaijan National Academy of Science is based on the legal regulations of the Republic of Azerbaijan. It includes data on (for example) student enrollment and retention, student performance and graduation, the composition of the University's student body, and on the University's research projects and output. Data will be identifiable or de-identified according to applicable legal requirements.

Reporting to the Ministry and the Academy is the responsibility of the Office of Admissions and Student Records and the Office of Faculty Affairs and Academic Administration.

h. Information for the general public, students, and other interested groups is published on the University's website and selectively supplied as printed and/or digital information material. It covers all areas necessary to provide a comprehensive picture of the University's academic performance, namely education, research, students and graduates, as well as faculty and staff. This includes data on (for example) student enrollment and retention, student performance and graduation, research output, graduate employment, and the composition of the University's body of students, faculty and staff. Unless classified as *public*, all data must be de-identified prior to publication. The publication of all relevant information on the University's website is the shared responsibility of the Office of Quality Assurance and Accreditation and the Office of IT and Information Services. Depending on the respective occasion and target group, printed and/or digital information material will also be provided by other administrative and/or academic units of the University.

i. On its website, in its Academic Catalogue, and by means of printed and/or digital information material, the University supplies further information intended to provide a broader picture of the University as an institution of higher education to the general public, students, and other interested groups. Since the information referred to in this case is non-personal in nature, it does not fall under the data usage and protection requirements outlined in this document. It includes (for example) a detailed overview of degree programs, learning outcomes, student admission and enrollment regulations, tuition fees, degree requirements, assessment regulations, and student support services. It generally covers all academic quality and quality assurance documents and altogether a wide variety of aspects of the University that are of significance to an interested audience. It is the shared responsibility of the Office of Quality Assurance and Accreditation and the Office of IT and Information Services to ensure that the University's website presents a comprehensive picture of the University. Responsibility for the Academic Catalogue rests with the Office of Admissions and Student Records. These Offices will cooperate with other academic and/or administrative units of the University whenever necessary.