جامعة الجميع الذكية

EVERYONE`S SMART UNIVERSITY

Privacy Policy

The main goal of applying the privacy policy to all university systems is to ensure the privacy of sensitive information about students; all employees are obligated to follow these policies:

1- Personal information defined as “any information about a person, including information that can be used to identify individuals, such as name, or used to follow and reach them, such as postal address and phone numbers, or any information that can be linked to individuals, such as medical records.

2- The university administration is responsible for the implementation of the policy and related documents, monitoring the application process, and acting appropriately in the case of non-commitment with it.

3- The Information Security Department reviews the policy and the extent to it is commitment, issues a report, at least once during the year.

4- This policy must be published directly after being approved by the university administration so that all users in Everyone’s Smart University can see it. The Information Security Department and the Information Technology Department shall send a notification to all users by all possible means. Users must also be notified in the event of a modification to the policy or the publication of any policy or supplementary document.

5- All users must comply fully with the terms of this agreement and all documents supporting it.

6- Receiving a notification concerning the availability of this policy to users or those who dealing with the university from inside or outside the university is an implicit notice of reading the policy with all its terms and implicitly agreeing to work on all its terms.

Types of personal information

- **Individual identification information**: It is the information that distinguish a particular individual, such as the full name, or any parts in any context that can indicate for a particular person, such as the national identity number, passport number and bank account number.
- **Individual follow-up information:** It is the information that can lead to a specific person, such as a postal address, personal email addresses, personal phone numbers of all kinds, and identification names on social networks.

7- Everyone's Smart University, represented by the Information Technology Department, will undertakes to make its maximum efforts and provide all necessary technologies and resources to protect personal information from deletion, damage, loss, leakage, modification, or any other unauthorized use.

8 - The Department of Information Security takes the responsibility for maintenance of a record of personal information, called the "Personal Information Directory", and one of the members of the information security team is going to be as the person responsible for protecting personal information.

9- The Personal Information Protection Officer shall be responsible for managing the directory.

10- The Personal Information Protection Officer shall be responsible for the validity of the information included in the Personal Information Manual on an ongoing basis, also for all audits to ensure that all systems and users follow the procedures and instructions contained in the Manual.

11- The Department of Information Technology at the university should provide the needed techniques and procedures to limit the locations of all forms of personal information on all information systems owned by the university.

12 - After the personal information is collected, it must be documented within the "Personal Information Directory", this includes:

Type of information: Individual identification information - Individual follow-up information and information sensitivity. All personal information at the university is classified according to its sensitivity in three categories: Low-sensitivity information - Medium-sensitive information and highly sensitive information.

13- The personal information directory shall include detailed information on all procedures used in collecting personal information, including:

- The reason behind collecting the information
- Method and procedure in collecting information.
- Details of the collected information and its classification

- The systems in which the information will be stored, it is preferable to define a unified copy of each type of personal information on a unified system, and copy or part of it to other systems when needed.
- Defining a specific owner of the information by the various business entities within the university, "Information Business Owner".
- Defining of a specific owner of the information by the "Information IT Owner".

All forms of information that is eligible to take, for example:

Database - Excel file - CSV text file - Information life cycle - Who has the right to access the information or part of it, and define the form of access - Who is entitled to authorize access to information, procedures for giving permission, and ways to document, monitor and audit those procedures.

14 - After listing personal information and documenting all information and procedures related to it in the "Personal Information Handbook", the Information Technology Department must redefine and rebuild the procedures for obtaining information.

15 - Procedure for collecting personal information: The procedure is going to be through an electronic form to achieve the following: The request for collecting personal information must mention all forms of its use, whether it is temporary or permanent and specifying the time of completion of use.

- The form must include detailed information on the required information.
- The form must include the method of accessing the information, whether it is access to the information through the system, or obtaining a copy of it.
- The form must include an undertaking to delete the information after achieving the goal.
- In case of obtaining a copy of the information, the application must recognize the form of obtaining the information.
- If personal information is requested to be shared with a third party, the form must include detailed information about that third party.
- In case that information is shared with one or more third parties, whether that party is from inside or outside the university, all parties must ensure that:

  - Fill out the form to obtain personal information.
  - In case the party requesting the information be from outside the university, written approval needed and the approval can be by sending an email sent from the address of the party requesting the information, and personal email addresses are not accepted.
  - The form must include an undertaking from the information collector to abide by the policy and procedures followed.
  - The form must include the approval of the Personal Information Protection Officer, and the approval of the Dean of Information Technology.

16 - The university has the right to extract demographic data from personal information, and use it to conduct statistical operations for the purposes of scientific research and administrative planning, without referring to users, if any data that could lead to the discrimination or tracking of individuals deleted.

17 - Any use of demographic data should be only after:

- Fill out the information request form.
- Recording the uses in the "Personal Information Directory".
- The personal information protection officer shall review the required data, to ensure that it is free from data that discriminates or tracks individuals.
- The approval of the Personal Information Protection Officer and the approval of the Dean of Information Technology.

In case of posting or sharing any personal information, must obtain the approval of the owners of the information before publishing the personal information.

18 - All users must have the ability to access and review their personal information to ensure its correctness. They must know the way to amend this information, either directly or by referring to the university staff

19 - The Personal Information Protection Officer is responsible for periodically checking the information to ensure its correctness and integrity if it is present on more than one system.

20 - The use of personal data should be minimum as much as possible in the testing and development processes, with guidance to use fictitious data for fictitious users as much as possible in the various testing processes that may be carried out by the IT teams or the rest of the organization's teams.

21- If personal information used for testing and development purposes, the form for collecting personal information must also be filled out.

22- Information technology personnel must be trained to deal with the personal data of users and preserve it, and the users must express their satisfaction in a written agree to the policy of dealing with personal data. This applies to all university employees whose work nature requires access to this information, directly or indirectly.

23 - Training on handling personal data should include training of employees on the procedures for creating an alert in the event of any breach of privacy.

24 - Defining clear procedures for dealing with privacy breaches, according to the classification of information suspected of leaking, this includes the date and time of the breach - Categories of users affected - Assessment of the damage and the risk that may result from it - Notifying information owners of the breaches - Escalation procedures must be followed.

25- Any personal data can be shared with other government agencies in the Kingdom of Saudi Arabia, by having an official letter.

26 - The Information Technology Department is responsible for defining a form of undertaking not to disclose information, which includes personal information, and to follow up on obtaining the written consent of all contracting companies and individuals on this form.

27- University websites can record information about users through the cookie technology without the explicit consent of the user; any use of the university's websites is an implicit consent to this policy and to the use of this technology.