Data Protection Policy

DATA PROTECTION POLICY

Department	**Academic Registry**	**Document No.**	**S07**
Document Type	**Data Protection Policy**	**Revision**	**1**
Owner	**Academic Registry**	**Pages**	**13**
Relevant to	**All OUC Students and Staff**		
Prepared by	**President and Executive Board Member** **Project and Compliance Lead**		
Reviewed by	**President and Executive Board Member** **Head of Student Experience and Academic Registry** **Project and Compliance Lead**		
Approved by	**President and Executive Board Member**		
Effective Date	**1st September 2022**		
Custodian	**Academic Registry**		

Revision History

Revision No.	Revision Date	Section No.	Reason of Revision
1.0	August, 2022		New Document

Dissemination

Through OUC Support Service Portal to all OUC staff and students.

Internal Control and Validation

To ensure compliance with this policy and procedure:

- The Dean, Academic Affairs is responsible for the implementation.
- The Academic Registry will maintain the control and compliance.

TABLE OF CONTENTS

1.1. POLICY OBJECTIVE **4**

1.2. DOMAIN OF IMPLEMENTATION **4**

1.3. DEFINITIONS **5**

1.4. ABBREVIATIONS **5**

1.5. GENERAL PRINCIPLES **5**

1.6. DATA PROTECTION PRINCIPLES **8**

1.7. COMPLIANCE WITH THE PRINCIPLES **8**

1.8. THE RIGHTS OF INDIVIDUALS **11**

1.9. SECURITY **11**

1.10. ACCOUNTABILITY AND GOVERNANCE **12**

1.11. DATA PROTECTION INFORMATION **13**

1.12. ADVICE AND INFORMATION **13**

1.1. Policy Objective

1.1.1. Oryx Universal College (OUC) collects, stores, and processes a wide range of data about individuals during its day-to-day business, and the use of personal data is an integral aspect of many of the College's activities.

1.2.1. This Policy outlines how we comply with the data protection obligations as set out by relevant laws of state of Qatar and how the college seeks to protect personal information relating to its staff, students, and other stakeholders.

1.3.1. The Policy is also to ensure that staff, students, and those who use or have access to, or custody of personal data held by the college understand and comply with the rules governing the processing of personal information which they may have access to during their period of employment and/or studies.

1.4.1. Processing means the "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available … or combination, restriction, erasure or destruction.

1.5.1. The Data Protection Law applies to all personal data processed by the College, or on behalf of the College, irrespective of where the data is held or in what format the data is held including paper, electronic and audio.

1.2. Domain of Implementation

1.2.1. The purpose of the DP Law is to protect the rights and privacy of individuals (referred to as 'Data Subjects') and to ensure that personal data is processed fairly, lawfully and transparently in compliance with the Data Protection Principles set out below at section 1.5.

1.2.2. This policy applies to all staff, students and others who use or have access to, or custody of, personal data which is in the control of the College. Any failure to do so may result in disciplinary proceedings.

1.2.3. All staff are responsible for ensuring the security of the personal data that they use or have access to as part of their role. It is a condition of employment that employees will abide by the rules and policies of the College.

1.3. Definitions

Special Categories Data	This means "personal data revealing racial or ethnic origin, relationships, criminal records, political opinions, religious or philosophical beliefs or trade union membership…. genetic data, biometric data…data concerning health or data concerning a natural person's sex life or sexual orientation".
Data Breach	A data breach is an incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner.
Data Retention	Data retention defines the policies of persistent data and records management for meeting legal and business data archival requirements.
Data Subjects	The individuals are the stakeholders who are either part of the organisation and anybody who is connected for business.

1.4. Abbreviations

OUC	Oryx Universal College
IAO	Information Asset Owners
DPO	Data Protection Officer
SIRO	Senior Information Risk Owner
CCTV	Closed-Circuit Television
GDPR	General Data Protection Regulation
DPIA	Data Protection Impact Assessment
DP	Data Protection

1.5. General Principles

1.5.1. Personal data

1.5.1.1. Under the DP Law personal data means "any information relating to an identified or identifiable living person".

1.5.1.2. Certain information referred to as 'Special Categories Data' is given more protection under the DP Law. Special Categories Data means "personal data revealing racial or ethnic origin, relationships, criminal records, political opinions, religious or philosophical beliefs or trade union membership…. genetic data, biometric data…data concerning health or data concerning a natural person's sex life or sexual orientation".

1.5.2. Data Protection Officer

1.5.2.1. The College has a Data Protection Officer who provides advice and guidance on data protection matters to the College.

1.5.2.2. The Data Protection Officer is located within Academic Registry Office and reports directly to the Head of Academic Registry and the Board of Directors.

1.5.2.3. The Data Protection Officer reports directly to our highest level of management and is given the required independence to perform their tasks.

1.5.2.4. We involve our Data Protection Officer, in a timely manner, in all issues relating to the protection of personal data.

1.5.2.5. The Data Protection Officer is sufficiently well resourced to be able to perform their tasks & OUC do not penalize the Data Protection Officer for performing their duties.

1.5.2.6. We ensure that any other tasks or duties we assign our Data Protection Officer do not result in a conflict of interests with their role as a Data Protection Officer.

1.5.3. Tasks for the role of DPO

1.5.3.1. DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

1.5.3.2. We will take account of our DPO's advice and the information they provide on our data protection obligations.

1.5.3.3. When carrying out a Data Protection Impact Assessment, we seek and take account of the advice of our DPO.

1.5.3.4. Our DPO acts as a contact point to co-operate, including prior consultations under the local laws, and will consult on any other matter.

1.5.3.5. When performing their tasks, our DPO has due regard to the risk associated with processing operations, and considers the nature, scope, context, and purposes of processing.

1.5.4. Senior Information Risk Owner (SIRO)

1.5.4.1. The Director – Digital Transformation is the College's SIRO and is responsible for the assurance of information security at OUC and for championing compliance with the Data Protection Law at the highest level.

1.5.5. Information Asset Owners (IAOs)

1.5.5.1. IAOs are the individuals across the college who are currently responsible for the main information systems and information assets.

1.5.5.2. Their role is to understand what information is held, what is added and what is removed, how information is moved and who has access and why.

1.5.5.3. They can understand and address risks to the information, know the vulnerabilities of the systems the data is stored in and ensure that information is processed in compliance with the DP Law.

1.5.6. Roles and Responsibilities

1.5.6.1. As well as the formal roles outlined above, all staff are responsible for the personal data that they process and have a duty to comply with the Data Protection Principles (set out below at section 1.6).

1.5.6.2. It is a condition of employment that all staff abide by the rules and policies of the college. Failure to do so may result in disciplinary proceedings.

1.5.6.3. Individuals who do not handle Personal Data as part of their normal work have a responsibility to ensure that any Personal Data they see or hear goes no further, e.g., data learned from a telephone call, contained on a computer print-out, or read on a computer screen.

1.5.6.4. OUC staff will pay particular attention to the enhanced requirements for the processing of Special Categories Data.

1.5.7. Training

1.5.7.1. The College aims to ensure that all staff are fully aware of their obligations under the DP Law and are aware of their personal obligations.

1.5.7.2. Data protection is a standing item on regular meetings, a set of policies and procedures to inform and guide staff as well as corporate communications to ensure a current awareness and consistency of message across the institution.

1.5.7.3. The College provides staff with adequate training in relation to their data protection responsibilities.

1.5.7.4. The College has a mandatory training programme which is signed off and endorsed by senior management. All those who use or have access to, or custody of personal data held by the College must complete the system training on a quarterly basis.

1.5.7.5. The content of the training programme is determined by the Information Security Manager and the Data Protection Officer to ensure it is appropriate and up to date.

1.5.7.6. Completion rates of the training will be reported regularly to the management as a standing agenda item and annually to the Board of Directors for Audit & for oversight and monitoring.

1.5.7.7. Failure to complete the training module may result in disciplinary action and/or loss of access to college systems.

1.6. Data Protection Principles

1.6.1. The Data Protection Principles ('the Principles'), as set out in the GDPR, provide a framework for processing personal data.

1.6.2. The principles state that personal data shall be:

1.6.2.1. processed **lawfully, fairly** and in a **transparent** manner.

1.6.2.2. collected for **specified, explicit** and **legitimate** purposes only, and **not** in a way that is **incompatible** with those purposes.

1.6.2.3. **adequate, relevant,** and **limited** to what is necessary in relation to the purposes for which they are processed (data minimization).

1.6.2.4. **accurate**, and where necessary**, kept up to date**. Every reasonable step must be taken to ensure that inaccurate personal data are deleted or corrected without delay.

1.6.2.5. kept in a form which permits identification for **no longer than necessary** for the purpose(s) for which the information is processed.

1.6.2.6. processed in a manner that ensures appropriate **security** of personal data, including protection against unlawful processing, and accidental loss, destruction, or damage.

1.6.3. OUC must be able to demonstrate compliance which each of the Principles. The Principles are regarded as the minimum standards of practice for any organisation processing personal data.

1.7. Compliance with the Principles

1.7.1. The College monitors and reviews its processing activities to ensure they are compliant with the DP Law.

1.7.2. The College follows the advice of the DPO and takes account of their knowledge regarding data protection obligations.

1.7.3. The College will undertake a Data Protection Impact Assessment, if appropriate, to identify and assess the impact on Data Subject's privacy because of amended or new means of processing personal data.

1.7.4. The College considers data protection and privacy issues upfront in everything that it does to ensure that it complies with the principles. It considers data protection issues as part of the design and implementation of systems, services, and business practices.

1.7.5. The College complies with the DP Law to allow Data Subjects to exercise their rights. It provides guidance to staff on how to recognise data rights requests and the process to follow on receipt.

1.7.6. The College affords extra protection to Special Categories and Criminal Convictions data and to data of those individuals in vulnerable groups.

1.7.7. Principle a) - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

1.7.7.1. OUC will ensure that personal data is only processed where a lawful basis applies and where processing is otherwise lawful.

1.7.7.2. Only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.

1.7.7.3. Ensure that data subjects receive full privacy information so that any processing of personal data is transparent.

1.7.7.4. All processing will be explained in privacy notices, targeted at & appropriate for different groups of data subjects, and usually be made available on our website.

1.7.7.5. The College only uses data processors that provide sufficient guarantees of their technical and organizational measures for data protection compliance.

1.7.7.6. Third parties with whom the College shares personal data or who process personal data on behalf of the College are expected to enter into formal agreements or contractual obligations which incorporate the requirements of the DP legislation.

1.7.8. Principle b) - Personal data shall be collected for specified, explicit & legitimate purposes & no further processed in a manner that is incompatible with the purposes.

1.7.8.1. OUC will only collect personal data for specified, explicit & legitimate purposes & will inform data subjects what those purposes are in a privacy notice.

1.7.8.2. Not use personal data for purposes that are incompatible with the purposes for which it was collected. If personal data is used for a new purpose that is compatible we will inform the data subject first.

1.7.9. Principle c) - Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

1.7.9.1. OUC will only collect the minimum personal data that is needed for the

purposes for which it is collected.

1.7.9.2. Ensure that the data it collects is adequate and relevant. All personal data held by OUC will be linked & recorded.

1.7.10. Principle d) - Personal data shall be accurate & where necessary, kept up to date.

1.7.10.1. OUC will ensure that personal data is accurate and kept up to date where necessary. Care will be taken where the use of the personal data has significant impact on individuals.

1.7.11. Principle e) - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

1.7.11.1. OUC will only keep personal data in identifiable form for as long as is necessary for the purposes for which it was collected or where we have a legal obligation to do so.

1.7.11.2. Once we no longer need the data it shall be deleted or rendered permanently anonymous. Retention limits are set out in Records Retention Schedule which all staff must abide by.

1.7.12. Principle f) - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing against accidental loss, destruction, or damage, using the appropriate technical or organizational measures.

1.7.12.1. OUC will ensure that there are appropriate technical or organizational measures in place to protect personal data.

1.7.13. Accountability - The data protection officer shall be responsible for and be able to demonstrate compliance with these principles.

1.7.13.1. OUC will ensure that records are kept of all personal data processing activities and these are provided to the competent authority on request.

1.7.13.2. OUC will always have an appointed Data Protection Officer.

1.8. The Rights of Individuals

The legislation provides the following rights for individuals:

1.8.1. To be informed

1.8.2. The right of access

1.8.3. The right to rectification

1.8.4. The right to erasure

1.8.5. The right to restrict processing

1.8.6. The right to data portability

1.8.7. The right to object and

1.8.8. Rights in relation to automated decision making and profiling

1.8.9. These rights do not apply in all circumstances.

1.9. Security

1.9.1. The College is committed to ensuring the security of personal data and has appropriate physical, technical and organizational measures in place including for example swipe card access to buildings and offices and password protected access to our networks and systems.

1.9.2. OUC staff who process personal data must ensure that it is always kept secure. The identity of an individual must be verified, particularly over the telephone, before disclosing any personal data. Processes for verifying identification will vary locally depending on the service and staff must follow the process in their area.

1.9.3. The College has policies and procedures in place relating to the security of data held electronically and all staff must ensure that they understand and abide by these.

1.9.4. Care must be taken to ensure that PC's and other devices which are used to view personal data are not visible to unauthorised persons, and particular attention must be taken in public spaces. Screens should not be left unattended, and staff should use the facility "lock" on their PC as appropriate.

1.9.5. In the case of manual data, files containing personal data must be kept securely in locked storage cabinets when not in use. Procedures should be in place to ensure that

the movement of files can be tracked. Files must not be left on desks overnight or during periods when offices or workspaces are unattended.

1.9.6. The College provides facilities for the confidential destruction of paper documents containing personal data and staff must ensure that they dispose of personal data using these facilities.

1.9.7. The College has set up a Digital Transformation Team to look at a technical solution for records storage, retention, and disposal. The aim is to align as fully as possible the data records, storage, and retention rates within OUCs information systems to enable the College to operate as efficiently and compliantly as possible with the DP Law.

1.9.8. The College processes CCTV footage in accordance with relevant legislation and code of practice & provides appropriate privacy notices where necessary. The College's CCTV Systems are available within the Security.

1.10. Accountability and Governance

1.10.1. The DPO retains the right to conduct audits and spot checks in relation to the processing of personal data and the College will hold staff to account for noncompliance with the Data Protection Principles and the Data Protection Policy.

1.10.2. The DPO will monitor and analyze trends in personal data breaches and data subject rights requests to understand themes and issues. Outputs will be reported to the management and included in an Annual Report to the Board of Directors.

1.10.3. Set up internal systems to receive and investigate complaints, data access requests, data correction or deletion requests and provide the data subjects with information relating to the same.

1.10.4. Set up internal systems for the effective management of personal data and report any violation of the same with the aim of safeguarding personal data.

1.10.5. Carry out comprehensive review and checking of the commitment to protect personal data.

1.11. Data Protection Information

1.11.1. If any parties are involved with OUC, requires more information on the data protection and its policy, data storage, or data related concerns can do so by contacting Academic Registry.

1.11.2. The request can be made by using their official [if organisation] or personal email to registry@oryx.edu.qa.

1.11.3. The requests made are reviewed and subject to other related policies and procedures.

1.12. Advice and Information

1.12.1. The OUC Academic Registry Staff are available to advise all on matters such as concerns about Data Usage, Transfer, etc. procedures. If anyone wish to contact, they can do so at Academic Registry.

1.12.2. Information on this Policy and Procedures are available on the College's Webpages at https://www.oryx.edu.qa/policies/ or by contacting the Academic Registry via telephone numbers +974 4021 0000 or via email at registry@oryx.edu.qa.

1.12.3. Further information and contact details are available on the College Web pages at https://www.oryx.edu.qa/.