Data Protection Policy for Research Activities

ORYX UNIVERSITY

In Partnership with Liverpool John Moores University

Document Reference:	RKEO-POL-Data Protection Research-V1.0
Version:	1.0
Effective Date:	14 February 2026
Review Cycle:	Annual
Next Review Date:	14 February 2027
Document Owner:	Director of Research and Knowledge Exchange
Responsible Office:	Research and Knowledge Exchange Office (RKEO)
Approved By:	University President

Version History

Version	Author	Description of Changes	Date
Version 1.0	Dr. Maher Salem	Created the first version	12 Feb 2026

Compliance Framework:

- Qatar Personal Data Privacy Protection Law (Law No. 13 of 2016)\
- GDPR principles (where applicable to international collaborations)
- LJMU Data Protection Policy

Table of Contents

1. Introduction

1.1 Purpose

This policy establishes the requirements for the protection of personal data in research activities conducted under the auspices of Oryx University. It ensures compliance with applicable data protection laws and aligns with the University's Research Ethics and Governance Framework.

1.2 Scope

This policy applies to:

- All research involving the collection, storage, processing, or sharing of personal data
- All staff, students, and affiliates conducting research
- All personal data regardless of format (electronic, paper, audio, video)
- Research conducted on-campus, off-campus, and internationally

1.3 Relationship to Other Policies

This policy should be read in conjunction with:

- Research Ethics Policy (**RKEO-POL-Research Ethics Policy**)
- Research Integrity Policy (**RKEO-POL-Research Integrity Policy**)
- University Data Protection Policy (institutional)
- Information Security Policy (institutional)

2. Legal Framework

2.1 Applicable Laws

Research data protection at Oryx University is governed by:

Jurisdiction	Legislation	Key Requirements
Qatar	Law No. 13 of 2016 on Personal Data Privacy	Consent-based processing; data subject rights; security requirements
Qatar Financial Centre	QFC Data Protection Regulations 2021	GDPR-aligned standards (if applicable to QFC entities)
International	Partner institution requirements (LJMU/UK GDPR)	May apply to collaborative research

2.2 Key Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person
Special Category Data	Sensitive personal data including health, genetics, biometrics, religion, political opinions, ethnicity, sexual orientation
Data Subject	The individual whose personal data is processed
Data Controller	The entity determining the purposes and means of processing (typically the University)
Data Processor	An entity processing data on behalf of the controller
Processing	Any operation performed on personal data (collection, storage, use, sharing, destruction)

3. Data Protection Principles

All research involving personal data must adhere to the following principles:

3.1 Lawfulness, Fairness, and Transparency

Requirement	Application to Research
Lawful basis	Identify and document the legal basis for processing (typically consent for research)
Fair processing	Do not process data in ways that would be unexpected or detrimental to participants
Transparency	Provide clear information about data processing in Participant Information Sheets

3.2 Purpose Limitation

Requirement	Application to Research
Specified purposes	Clearly define research purposes at the outset
Compatible use	Further processing must be compatible with original purposes
Research exemption	Further processing for research purposes is generally considered compatible

3.3 Data Minimization

Requirement	Application to Research
Adequate	Collect sufficient data to meet research objectives
Relevant	Only collect data necessary for the research
Limited	Do not collect data "just in case" it might be useful

3.4 Accuracy

Requirement	Application to Research
Accurate data	Take reasonable steps to ensure data accuracy
Correction	Have processes to correct inaccurate data
Verification	Consider verification procedures for critical data

3.5 Storage Limitation

Requirement	Application to Research
Retention periods	Define and document retention periods
Justification	Justify retention periods based on research needs and legal requirements
Destruction	Securely destroy data when no longer needed

3.6 Integrity and Confidentiality (Security)

Requirement	Application to Research
Technical measures	Encryption, access controls, secure storage
Organizational measures	Training, policies, procedures
Risk-based approach	Security proportionate to risk

3.7 Accountability

Requirement	Application to Research
Demonstrate compliance	Document data protection measures
Records of processing	Maintain records of research data processing activities
Responsibility	Clear assignment of data protection responsibilities

4. Legal Bases for Research

4.1 Consent

Consent is the most common legal basis for research data processing.

Requirements for Valid Consent:

Element	Requirement
Freely given	No pressure or negative consequences for refusing
Specific	Consent for specific, defined purposes

Informed	Full information provided before consent
Unambiguous	Clear affirmative action (signature, checkbox)
Documented	Written record of consent
Withdrawable	Easy to withdraw as to give

4.2 Other Legal Bases

Legal Basis	When Applicable	Considerations
Legitimate Interests	When consent is impractical and processing is necessary for research	Requires documented Legitimate Interests Assessment
Public Interest	Research in the public interest	Must be recognized in law; typically for public institutions
Legal Obligation	Required by law	Rare in research context

4.3 Special Category Data

Processing special category data requires:

- A legal basis from Section 4.1/4.2 above, AND
- An additional condition, typically **explicit consent** for research

Additional Safeguards for Special Category Data:

- Explicit consent (not just standard consent)
- Data Protection Impact Assessment (DPIA)
- Enhanced security measures
- Minimization of identifiable data
- Pseudonymization where possible

5. Data Subject Rights

5.1 Rights Overview

Right	Description	Research Implications
Right to be Informed	Know how data is used	Addressed through Participant Information Sheet
Right of Access	Obtain copy of their data	Must be able to retrieve and provide data
Right to Rectification	Correct inaccurate data	Must have process for corrections
Right to Erasure	Request deletion of data	May be limited for research purposes

Right to Restrict Processing	Limit how data is used	Must be able to implement restrictions
Right to Data Portability	Receive data in portable format	Applies to automated processing based on consent
Right to Object	Object to processing	Must consider and respond to objections

5.2 Research Exemptions

Some rights may be limited for research purposes where:

- Processing is necessary for research in the public interest
- Exercise of the right would seriously impair the research
- Appropriate safeguards are in place

Exemptions must be:

- Applied on a case-by-case basis
- Documented and justified
- Communicated to participants in advance where possible

6. Data Security

6.1 Security Requirements by Data Type

Data Classification	Security Requirements
Anonymous Data	Standard security; password-protected storage
Pseudonymized Data	Encrypted storage; key stored separately; access controls
Identifiable Data	Encrypted storage; strict access controls; audit logging
Special Category Data	All above plus enhanced encryption; minimal retention; DPIA

6.2 Technical Security Measures

Measure	Requirement
Encryption	AES-256 or equivalent for data at rest; TLS 1.2+ for data in transit
Access Controls	Role-based access; principle of least privilege
Authentication	Strong passwords; multi-factor authentication for sensitive data
Backup	Regular encrypted backups; tested recovery procedures
Audit Logging	Log access to identifiable/sensitive data
Endpoint Security	Antivirus; firewall; automatic updates

6.3 Organizational Security Measures

Measure	Requirement
Training	All researchers complete data protection training
Policies	Clear policies and procedures documented
Access Management	Formal process for granting/revoking access
Incident Response	Documented breach response procedures
Third Party Management	Due diligence on processors; contracts in place

6.4 Approved Storage Locations

Acceptable	Not Acceptable
University secure servers	Personal devices (unless encrypted and approved)
University-approved cloud (Microsoft 365, approved research platforms)	Consumer cloud services (personal Dropbox, Google Drive)
Encrypted external drives (for backup only)	Unencrypted USB drives
Secure filing cabinets (paper documents)	Unlocked storage

7. Data Sharing

7.1 Internal Sharing

Sharing within the University research team:

- Limited to those who need access for research purposes
- Documented in data management plan
- Subject to confidentiality obligations

7.2 External Sharing

Sharing with external parties requires:

Requirement	Details
Legal basis	Consent or other lawful basis for sharing
Data Sharing Agreement	Formal agreement specifying terms, responsibilities, security
Due diligence	Assessment of recipient's data protection capabilities
Participant information	Participants informed of sharing in advance
Minimization	Share minimum necessary data; anonymize where possible

7.3 International Transfers

Transfer of personal data outside Qatar requires:

Safeguard	Description
Adequacy	Transfer to country with adequate data protection laws
Standard Contractual Clauses	Approved contractual terms with recipient
Consent	Explicit consent for transfer (inform of risks)
Binding Corporate Rules	For transfers within corporate group

8. Data Retention and Destruction

8.1 Retention Periods

Data Type	Minimum Retention	Maximum Retention	Notes
Research data (general)	10 years from publication	As specified in consent	Funder requirements may vary
Clinical/health research	15 years	Per regulatory requirements	May be longer for certain studies
Student projects (UG)	2 years after completion	5 years	
Student projects (PGT)	3 years after completion	5 years	
Student projects (PGR)	10 years after completion	As specified	Aligned with publication requirements
Consent forms	Duration of data retention + 1 year	Same as data	Evidence of consent

8.2 Retention Justification

Retention periods must be:

- Documented in data management plan
- Communicated to participants
- Justified by research needs, legal requirements, or funder policies
- Reviewed periodically

8.3 Secure Destruction

Data Format	Destruction Method

Paper documents	Cross-cut shredding (DIN 66399 Level P-4 or above) or confidential waste service
Electronic files	Secure deletion software (multiple overwrites) or IT Services assistance
Hard drives/storage media	Physical destruction or degaussing
Audio/video recordings	Secure deletion after transcription (if applicable)
Cloud storage	Permanent deletion; verify removal from backups
Email	Permanent deletion from all folders including trash

8.4 Destruction Documentation

Maintain records of:

- What was destroyed
- When destruction occurred
- Method of destruction
- Who authorized destruction
- Who performed destruction

9. Data Protection Impact Assessment (DPIA)

9.1 When Required

A DPIA is required when research is likely to result in high risk to individuals, including:

Trigger	Examples
Large-scale processing of special category data	Health data from many participants
Systematic monitoring	Tracking behaviour over time
Vulnerable populations	Children, patients, prisoners
New technologies	AI, biometrics, genetic analysis
Profiling or automated decisions	Algorithms affecting individuals
Cross-border transfers to non-adequate countries	Data sent to countries without strong protection
Combining datasets	Linking data from multiple sources

10. Data Breaches

10.1 Definition

A personal data breach is a security incident leading to:

- Accidental or unlawful destruction, loss, or alteration of personal data
- Unauthorized disclosure of or access to personal data

10.2 Examples in Research Context

Type	Examples
Confidentiality breach	Unauthorized access; data sent to wrong recipient; lost device
Integrity breach	Unauthorized alteration of data
Availability breach	Data lost or destroyed; ransomware

10.3 Breach Response Procedure

The following is a Data Breach Response Procedure Summary tables which explain the process in detail.

PHASE 1: IMMEDIATE RESPONSE (`Within 24 hours`)

Step	Action	Key Activities	Responsible Parties
1	CONTAIN	Stop breach, if possible, isolate affected systems, secure access	IT Security, System Administrators
2	REPORT	Notify IT Security AND Data Protection Officer immediately	Anyone detecting breach
3	DOCUMENT	Record what happened, when, what data affected, initial assessment	Incident Lead, IT Security

PHASE 2: ASSESSMENT (`Within 48 hours`)

Step	Action	Key Activities	Risk Categories
4	ASSESS	Determine scope, root cause, impact assessment, risk level	All levels: High/Medium/Low
5	CATEGORIZE	Classify risk level to individuals based on data sensitivity and impact	**High Risk**: Sensitive personal data **Medium Risk**: Limited personal data **Low Risk**: Anonymous/anonymized data

PHASE 3: NOTIFICATION (`Within 72 hours if HIGH RISK`)

Step	Action	Recipients	Criteria/Requirements
6	REGULATOR NOTIFICATION	Supervisory authority (Qatar Data Protection)	Mandatory for high-risk breaches, within 72 hours of assessment
7	INDIVIDUAL NOTIFICATION	Affected research participants	Required for high-risk breaches, UREC must review notification text
8	UREC NOTIFICATION	University Research Ethics Committee	All breaches affecting research participants

PHASE 4: REMEDIATION (Ongoing)

Step	Action	Key Activities	Outcomes
9	INVESTIGATE	Root cause analysis, forensic examination	Understanding of why breach occurred
10	REMEDIATE	Implement corrective measures, security patches	Vulnerabilities addressed, systems secured
11	REVIEW	Update security procedures, controls, training	Improved procedures to prevent recurrence
12	DOCUMENT	Complete breach log, lessons learned, final report	Institutional knowledge, compliance record

RISK CATEGORIZATION MATRIX

Risk Level	Criteria	Notification Required
HIGH	Sensitive personal data (health, biometrics, financial), large scale breach, potential harm to individuals	Yes - to regulator AND individuals
MEDIUM	Limited personal data, minimal risk of harm, contained breach	May require regulator notification
LOW	Anonymous/anonymized data, no risk to individuals, minor incident	Internal documentation only

TIMELINE SUMMARY

Phase	Timeframe	Key Deadline
Immediate Response	0-24 hours	Containment and initial reporting
Assessment	24-48 hours	Risk categorization completed
Notification	48-72 hours	Regulator notification if high risk
Remediation	Ongoing	Continuous improvement

KEY CONTACTS

Role	Contact Method	Responsibility
IT Security Team	security@oryx.edu.qa / +974 xxxxx	Technical containment, investigation
Data Protection Officer	dpo@oryx.edu.qa / +974 xxxxxx	Regulatory compliance, oversight
UREC Chair	rkeo@oryx.edu.qa / +974 xxxxx	Research participant protection

DECISION POINTS

Decision	Criteria	Action
Fast-Trackvs Full Review	Based on risk categorization	High risk → Full committee review
Notification Required?	High risk classification	Notify regulator within 72 hours
Participant Notification?	High risk to individuals	Notify with UREC-approved message

UREC Involvement	Any research participant data affected	Mandatory UREC notification

10.4 Breach Notification Content

Notification to individuals must include:

- Description of the breach
- Name and contact details of DPO
- Likely consequences of the breach
- Measures taken to address the breach
- Measures individuals can take to protect themselves

11. Roles and Responsibilities

Role	Data Protection Responsibilities
University (Data Controller)	Overall accountability for data protection compliance
Data Protection Officer (DPO)	Advises on compliance; monitors implementation; point of contact for regulators and individuals
Director of Research and Knowledge Exchange	Ensures research-specific data protection policies and procedures; liaison with DPO
UREC	Reviews data protection aspects of ethics applications; monitors compliance
Principal Investigators	Responsible for data protection in their research; implement appropriate measures
All Researchers	Comply with this policy; complete training; report breaches
IT Services	Provide secure infrastructure; support security measures

12. Training Requirements

Audience	Training Required	Frequency
All researchers (staff)	Data Protection in Research module	On appointment; refresher every 2 years
PGR students	Data Protection in Research module	On registration; before data collection
PGT/UG students (research projects)	Data Protection basics	Before project begins
UREC members	Enhanced data protection training	On appointment; annual refresher

Research Office staff	Data Protection in Research + Advanced	On appointment; annual refresher

13. Compliance and Enforcement

13.1 Monitoring

Compliance is monitored through:

- UREC review of ethics applications
- Periodic audits of research data handling
- Incident and breach reporting
- Annual compliance reporting

13.2 Non-Compliance

Failure to comply with this policy may result in:

- Requirement for additional training
- Suspension of research activities
- Withdrawal of ethics approval
- Disciplinary action
- Reporting to regulatory authorities

14. Review

This policy will be reviewed annually and updated to reflect:

- Changes in data protection legislation
- Regulatory guidance
- Best practice developments
- Lessons learned from incidents