Knowledge UNIVERSITY

Data Protection and Privacy Policy

2026–2027

Policy and implementation procedures

KNU DP 01 | Version 1.0

Prepared for institutional adoption

Erbil | Kurdistan Region of Iraq

Table of Contents

This policy combines institutional rules with the procedures and forms needed to put them into practice. The main policy is suitable for publication. Completed forms, system information and individual case records must be stored separately with controlled access.

Table of Contents	Page
Document guide and adoption rules	2–3
1 Purpose scope and definitions	4
2 Principles and permitted processing	5
3 Accountability and responsibilities	6
4 Collection transparency and sensitive information	7
5 Access and information security	8
6 Academic records research and support services	9
7 Sharing suppliers and international transfers	10
8 Individual requests and complaints	11
9 Data incidents and breach response	12
10 Retention disposal and legal holds	13
11 Assurance training and implementation	14
Appendix A Student privacy notice	15
Appendix B Employee privacy notice	16
Appendix C Retention schedule	17
Appendix D Data inventory and risk assessment	18
Appendix E Access and confidentiality forms	19
Appendix F Request and incident forms	20
Appendix G Adoption evidence and references	21

KNOWLEDGE UNIVERSITY

Erbil | Kurdistan Region of Iraq

Data Protection and Privacy Policy

2026-2027

Employees students and institutional records

Policy and implementation procedures
Version 1.0 •

Knowledge University protects the personal information entrusted to it throughout admission, study, employment, research and university services. This document sets the rules, responsibilities and practical procedures for doing so.

Document control	Detail
Policy reference	KNU DP 01
Scope	All colleges, departments, centres, personnel and service providers handling University personal data
Policy owner	Directorate of Quality Assurance and Accreditation
Executive accountability	University President
Approval route for adoption	University Council endorsement and President authorisation, subject to the University's delegated authority
Status	Prepared for institutional adoption; not evidence of approval or implemented controls
Effective date	Date of authorised approval recorded below
Review cycle	Annually from approval, or sooner after material change or a serious incident
Classification	Public policy; completed operational records are Confidential or Restricted

Approval record

Decision reference _____ Approval date _____
Authorised signatory _____ Signature _____

The approval record must be completed from an actual institutional decision. The operational requirements and time targets below take effect on approval; existing implementation must be verified through the adoption checklist.

How this document is to be adopted

Approval adopts the internal rules and service targets in this document. It does not certify compliance or retrospectively create records. The President must confirm the approval route, allocate resources and commission a check of applicable legal and Ministry requirements before implementation. Any stricter binding requirement takes precedence and must be recorded in the compliance register.

1 Purpose scope and definitions

1.1 Policy commitment

Knowledge University shall collect and use personal information only for a defined, justified and authorised purpose. It shall protect confidentiality, integrity and availability; explain relevant uses; maintain accurate records; and restrict retention and disclosure to what is necessary. Staff shall treat privacy as part of their academic and professional duties.

1.2 Scope

This policy applies to applicants, enrolled and former students, all employees and applicants for employment, academic and administrative staff, visiting and part-time personnel, contractors, volunteers, research participants and other individuals whose information the University handles. It applies on and off campus, to paper and electronic files, email, ERP and learning systems, websites, recordings, mobile devices, backups and approved cloud services.

1.3 Key definitions

- Personal data means information identifying a living person directly or indirectly, including identity numbers, contact details, employment records, marks, images and online identifiers.
- Sensitive data means information requiring greater protection, including health and counselling information, disability, biometrics, allegations, disciplinary matters and information revealing personal beliefs or other highly private circumstances.
- Processing includes collecting, consulting, recording, organising, sharing, changing, retaining and destroying information.
- A data owner is the head of the unit accountable for a defined record set. A processor or service provider handles information on the University's instructions.
- A data incident is suspected or actual loss, unauthorised access or disclosure, alteration, destruction or unavailability of personal data. Pseudonymised records remain personal data where people can be reidentified.

1.4 Legal and accreditation context

The University shall comply with applicable Iraqi and Kurdistan Region laws, Ministry instructions, contractual commitments and professional obligations. Article 17 of the Iraqi Constitution recognises personal privacy. ASIC University Standard A.10.1 requests procedures and protocols protecting employee and student data. These references support this policy; they do not replace an assessment of specific legal duties.

The policy uses recognised privacy principles as institutional commitments. UK or EU data protection rules shall not be described as automatically applicable merely because the University seeks ASIC accreditation. The designated lead shall obtain qualified advice where a particular activity, overseas relationship or law may create additional obligations.

2 Principles and permitted processing

2.1 Mandatory principles

- Fairness and transparency. Explain significant uses in clear language and avoid unexpected or misleading processing.
- Purpose limitation. Use information for the recorded purpose. Review a new or materially different purpose before it begins.
- Minimum necessary data. Collect only relevant fields and limit the people, recipients and copies involved.
- Accuracy. Provide a route for correction and check critical identity, employment and assessment information before decisions.
- Limited retention. Apply the approved schedule and stop deletion when a legal hold is issued.
- Security and accountability. Use safeguards proportionate to risk, assign owners and retain evidence of decisions.

2.2 Authorised grounds and purposes

Before processing begins, the data owner shall record its purpose, necessity and applicable authority or justification. This may include a binding legal or Ministry requirement; admission, education or employment arrangements; an authorised institutional function with proportionate privacy safeguards; protection of life or safety; or freely given consent where appropriate. These are institutional decision categories, not a representation that a foreign statutory framework applies.

Routine purposes may include admissions and registration, teaching and assessment, awards verification, payroll and employment administration, financial transactions, student support, campus security, approved research, service administration and quality assurance. A legitimate institutional purpose does not authorise unrestricted access or publication.

2.3 Consent and optional uses

Consent shall be specific, informed, recorded and capable of withdrawal without inappropriate disadvantage. Optional publicity, identifiable testimonials and nonessential marketing shall not be bundled with enrolment or employment. Refusal shall not affect teaching, assessment, recruitment or employment decisions. Withdrawal stops future consent-based use; unavoidable limitations concerning material already distributed must be explained.

2.4 Prohibited practices

Staff shall not sell personal data, browse records out of curiosity, share credentials, circulate identifiable marks in open groups, disclose salaries or health records without authority, or export records into personal email or unapproved storage. Blanket consent shall not substitute for an appropriate processing justification.

3 Accountability and responsibilities

Approval of this policy assigns the following responsibilities by office. These assignments are policy provisions for adoption, rather than a claim that a statutory data protection officer has already been appointed.

Office or role	Required responsibility
President	Ensure resources and accountability; authorise high-risk decisions and exceptions; require corrective action and escalation.
Directorate of Quality Assurance and Accreditation	Own the policy and act as designated data protection coordination lead on adoption; maintain request, incident, risk and compliance registers; report to the President.
IT function	Implement technical controls, access changes, logging, backups and restoration; support incident containment and supplier assessment.
HR function	Own personnel and recruitment records; verify employment disclosures; coordinate joining, role changes and leaving procedures.
Student Registration function	Own admissions and official student records; verify student identity; control transcript and award disclosures.
Deans directors and heads	Own local records; approve minimum access; keep inventories; supervise retention, training and corrective action.
Research Center and relevant ethics reviewers	Review research data arrangements, participant information, sensitive uses and approved sharing.
Finance and procurement functions	Protect financial records; ensure supplier agreements and payment processes meet this policy.
All staff and authorised users	Use information only for assigned duties; complete training; protect records; report suspected incidents immediately.

3.1 Coordination and independent review

Each unit shall nominate a contact to support the designated lead. The President shall appoint an alternative reviewer where the lead has a conflict, is personally involved in a complaint or would be reviewing their own decision. The lead shall have access to management and appropriate legal or technical advice.

3.2 Contact and escalation

Address privacy correspondence to the Directorate of Quality Assurance and Accreditation, Knowledge University, Erbil, Kurdistan Region of Iraq. Requests may be delivered through the Presidency office or Student Registration for confidential routing. Presidency telephone: +964 750 3000 800. Registry: +964 750 3000 600 or +964 750 3000 700. Use calls to arrange secure submission; do not transmit sensitive documents to an unverified recipient.

4 Collection transparency and sensitive information

4.1 Collecting information

The data owner shall approve forms and specify mandatory and optional fields. At collection, explain the responsible University unit, purpose, relevant recipients, retention approach, consequences of withholding required information and the request or complaint route. If information comes from another source, record the source and provide appropriate notice unless a binding rule or documented justified restriction prevents it.

Privacy notices in Appendices A and B shall be made available at admission, recruitment and onboarding, and on the University website after adoption. Special activities shall receive an additional notice where their use or risk differs materially. Notices must accurately reflect actual services and suppliers. They must not promise a control or practice that has not been implemented.

4.2 Sensitive records

Health, disability, counselling, disciplinary and other sensitive files shall be separated from general student or staff files and restricted to specifically authorised personnel. Routine teaching and managerial records shall contain only the support adjustment or decision needed, rather than detailed clinical or counselling histories. Any disclosure for an urgent safety concern must be necessary, limited and documented.

4.3 Children and vulnerable individuals

Where an applicant, student or research participant is a minor or requires additional support, the responsible unit shall assess applicable consent and representation requirements, provide understandable information and verify the authority of a parent or representative. A family relationship alone shall not justify access to a student’s records. Staff shall consider safety, confidentiality and applicable legal obligations before disclosure.

4.4 Images recordings and monitoring

Identifiable promotional photographs, interviews and testimonials require documented permission or another clearly recorded and justified basis, with an effective route to raise objections. Obtain separate permission for an identifiable featured subject. Do not publish personal contact details, IDs, signatures or private marks with activity news.

CCTV, attendance monitoring, online proctoring and any biometric tool require a documented necessity and privacy risk assessment. Give appropriate notice, limit locations and access, and prohibit cameras in toilets, changing areas and private counselling spaces. Audio recording or a new biometric system requires specific President authorisation following legal and risk review. No solely automated decision with significant academic or employment effect may be made without meaningful human review and a challenge route.

5 Access and information security

5.1 Access lifecycle

The data owner shall approve named-user access specifying the system, record set, role, purpose and expiry where relevant. IT shall issue individual accounts and record approvals. Access shall follow least privilege; administrative access shall be separate from ordinary work accounts. Shared credentials are prohibited. Where a service cannot support individual accountability, IT must document compensating controls and obtain a time-limited exception.

Review privileged and sensitive-record access at least quarterly and all other access at least annually. HR and line managers shall notify IT before a planned departure or role change. Disable access by the effective leaving time, immediately for an urgent security suspension, and remove obsolete permissions on a role change. Transfer business records securely before removing an account.

5.2 Minimum technical controls

- Use multi-factor authentication for privileged, remote, email and cloud access wherever supported; record exceptions and remediation dates.
- Use unique strong passwords or passphrases, secure recovery and prompt changes after compromise. Lock unattended screens and protect devices with encryption where supported.
- Keep supported software updated; use endpoint protection and secure configurations. Restrict exports and public links; encrypt confidential data in transit and on portable media.
- Log significant access and changes to sensitive systems; protect logs against alteration and limit who can consult them. Review relevant logs during incidents and scheduled assurance checks.
- Maintain protected backups of critical systems, with a separate or isolated copy. Define recovery priorities and test restoration at least quarterly. Document recovery time and data-loss tolerances for each critical service.

5.3 Paper remote work and communications

Keep confidential paper records in locked storage with controlled keys. Use a clear desk approach, collect printing promptly and use confidential waste disposal. Record significant file transfers and do not leave records in vehicles or public areas. Personal devices may access data only with IT approval, adequate security and a method for removing University information on loss or departure.

Use approved institutional communication and storage. Verify recipients and attachments before sending, use BCC for unrelated recipients and secure links for sensitive files. Send any decryption password separately. Personal messaging groups shall not be used to share identifiable grades, HR files or health information.

6 Academic records research and support services

6.1 Teaching assessment and quality assurance

Lecturers shall access only the classes and records assigned to them. Communicate individual marks through authenticated systems or a verified private channel. Examination papers, scripts, marking keys and marks shall have restricted storage, controlled transfer and an audit trail for changes. Verify a student's identity before releasing results or transcripts. Public posting shall not reveal personal results without an approved justification and safeguards.

Course files, teacher portfolios, student feedback and accreditation evidence shall contain the minimum personal information required. Use anonymised or redacted samples where possible. Student feedback reporting shall avoid exposing respondents, particularly in small groups. Staff shall not place identifiable disciplinary, counselling or health material in routine course folders.

6.2 Research and scholarly activity

Before collecting participant data, the responsible researcher shall secure applicable ethics approval and prepare a data management plan covering purpose, notice or consent, storage, access, sharing, retention and destruction. Separate participant identifiers from research datasets and limit access to the linking key. Approval for publication does not automatically permit release of identifiable raw data.

Research involving health information, children, vulnerable groups, linkage of datasets or international sharing requires documented additional review. Agreements shall establish ownership, confidentiality, permitted use and end-of-project arrangements. Anonymisation shall be tested for reidentification risk; removing names alone is insufficient.

6.3 Counselling clinical and support services

The Psychosocial Counseling Center and any clinical or health-related service shall maintain restricted case records. Routine referral shall share only information necessary for the service. Disclosure to teaching staff shall normally describe agreed support rather than clinical detail. Professional duties and applicable legal or safety exceptions shall be explained to the individual and recorded when used.

6.4 Websites artificial intelligence and digital tools

Website and form owners shall minimise collected fields, display an appropriate privacy notice and limit access to submissions. IT shall review website tracking and third-party integrations; optional tracking requires an appropriate choice mechanism where applicable. Public staff profiles shall contain approved professional information.

Staff shall not enter identifiable student, employee, patient or research participant data, confidential examination materials or credentials into public AI tools. Any approved AI or analytics service handling personal information requires prior risk, contract and security review. Training or reuse of University data by a provider must be explicitly controlled in the agreement.

7 Sharing suppliers and international transfers

7.1 Internal and external disclosure

Share information only with a recipient who needs it for an authorised purpose. Verify identity and authority, limit fields, select a secure channel and record significant disclosures. Requests from relatives, employers, agents or sponsors require valid authority or a documented applicable obligation. Staff shall not confirm attendance, marks or employment details merely because the requester knows the individual.

Requests from courts, law enforcement, Ministries or regulators shall be referred to the President and designated lead for verification and, where needed, legal advice. Preserve relevant records. Document the request, applicable authority, information disclosed, recipient and approving officer. Do not obstruct a binding requirement or disclose more than it authorises.

7.2 Accreditation and partnership evidence

For ASIC and other external reviews, provide anonymised or redacted evidence first. Where identifiable information is necessary, establish the inspection purpose, authorised reviewers, secure access arrangements and retention or return terms. Inspection access shall not include routine access to full personnel files, counselling files or unrestricted system accounts. Record access and remove temporary permissions after the review.

7.3 Supplier due diligence and contracts

Before using an external platform, cloud service or contractor, the data owner, IT and procurement shall review the information involved, hosting locations, access controls, security history and incident support. The contract shall address:

- Documented instructions, permitted purposes and confidentiality obligations.
- Security standards, subcontractor approval and the countries where data may be stored or accessed.
- Prompt incident notification, cooperation with requests and investigations, and sufficient evidence of compliance.
- Return or secure deletion at termination, including the treatment of backups and a deletion confirmation.
- Audit or assurance rights, continuity arrangements and restrictions on advertising, sale or provider model training.

7.4 International access and transfer

Overseas hosting, remote support, exchange programmes and research collaboration may create an international transfer. Before transfer, the designated lead shall assess applicable law and contractual obligations, destination risks, recipient safeguards and individual notices. The President or authorised delegate shall approve the arrangement. Record the decision, minimise identifiers and protect transmission. Where protections are insufficient, do not proceed until an acceptable alternative is established.

8 Individual requests and complaints

8.1 Available requests

Students, employees and other individuals may ask what personal information the University holds, seek a copy, request correction, question a disclosure, withdraw consent for an optional use, or request restriction or deletion where appropriate. These routes are University commitments subject to applicable legal requirements. Deletion is not automatic where the University must retain reliable academic, employment, financial or dispute records.

8.2 Receipt and verification

Requests may be submitted in writing, in person or through a representative to the designated lead, Student Registration, HR or the Presidency office. No special form is mandatory. The receiving unit shall forward the request securely within one working day. Record the receipt date, scope and requested communication method. Acknowledge within five working days and verify identity using proportionate checks; avoid retaining unnecessary copies of identity documents.

8.3 Search review and response

The designated lead shall allocate the search to relevant data owners, including email and paper records where in scope. Data owners shall preserve responsive records, identify third-party information and return the search outcome securely. The lead shall review applicable restrictions, confidentiality and any redactions before issuing an intelligible response. Secure delivery and recipient verification are mandatory.

The University target is a substantive response within 30 calendar days of receipt. Seek clarification promptly if needed and explain how it affects the search. Where a complex request cannot be completed within this target, explain the reason and revised date before the deadline and record the decision. A shorter binding legal deadline takes precedence. Internal targets do not create an automatic legal extension.

8.4 Corrections refusals and record integrity

Correct verified errors promptly, retain an appropriate audit trail and inform relevant recipients where feasible. A request to change an academic judgement shall follow the academic appeal process; it shall not be treated as permission to overwrite the original result. If a request is refused wholly or partly, explain the reasons, applicable authority and review route without revealing protected information.

8.5 Complaints and independent escalation

A person may complain to the designated lead without retaliation. Acknowledge within five working days and aim to provide an outcome within 30 calendar days. An unresolved complaint, or one concerning the lead, may be escalated to the President for an independent reviewer. Preserve the person’s right to use any competent external authority or legal remedy applicable to the matter. Record the complaint, investigation, outcome and corrective actions.

9 Data incidents and breach response

9.1 Immediate reporting

All users shall report an actual or suspected incident immediately to IT and the designated lead through a verified institutional channel. If these contacts are unavailable, contact the Presidency office on +964 750 3000 800 for urgent routing. Do not delay reporting while trying to prove a breach or complete a form. Report lost devices, misdirected email, missing paper files, exposed links, account compromise and ransomware.

9.2 Contain and preserve

IT and the record owner shall limit further exposure: revoke public links, suspend compromised accounts, isolate affected equipment and retrieve misdirected information where possible. Preserve logs and other evidence. Do not delete evidence, pay demands or contact an attacker without authorised direction. A person may take an immediate safe action within their competence, but must not conduct an unauthorised investigation.

9.3 Assess and escalate

The designated lead shall open an incident record and coordinate an initial assessment with IT and the owner as soon as practicable, with a target of 24 hours from awareness. Record the data and individuals involved, sensitivity, extent of exposure, likely harm, recovery options and whether further disclosure remains possible. Escalate immediately to the President where sensitive data, many individuals, fraud, safety risks or critical system disruption are involved.

9.4 Notification decision

The President, supported by the lead and qualified advice where necessary, shall determine whether notification to affected people, competent authorities, partners or other parties is required by applicable law, contract or risk. Record the grounds and timing for notification or non-notification. Meet any applicable mandatory deadline; there is no universal 72-hour legal deadline assumed by this policy.

Where notification is required, communicate without undue delay through a secure and accessible channel. Explain what happened, relevant information types, likely consequences, actions taken, steps the person can take and a contact for assistance. Avoid speculative claims, unnecessary identifiers or instructions that expose the person to further harm.

9.5 Recovery and closure

IT shall verify safe restoration; the owner shall confirm integrity of affected records. Assign corrective actions, owners and dates. The designated lead shall conduct a lessons review normally within ten working days of stabilisation and monitor action completion. Keep every incident in the register, including near misses. Do not state that no incidents occurred merely because a register has not previously been maintained.

10 Retention disposal and legal holds

10.1 Retention rules

Each record set shall have an accountable owner, a documented retention trigger, a period and a final action. Appendix C establishes internal default periods for adoption. They are policy choices, not verified statutory periods. Before deletion, the owner and designated lead shall check the compliance register for applicable Ministry, legal, funding, contractual and professional requirements. A longer binding period prevails; indefinite retention requires a defined justification and periodic review.

Retain the authoritative record and eliminate unnecessary duplicates. Do not keep copies in personal accounts, forgotten exports or unofficial folders. Where a dataset is needed only for statistical analysis, use effective anonymisation rather than retaining identifiers indefinitely.

10.2 Legal holds

Suspend normal disposal where a complaint, appeal, audit, investigation, legal claim or preservation notice affects the records. The President or designated lead shall issue a hold identifying scope, owners, start date and review arrangements. Owners shall protect originals and relevant copies, acknowledge the instruction and prevent routine deletion. Only the issuing authority or an authorised replacement may release a hold in writing after checking continuing obligations.

10.3 Secure destruction

The owner shall review records due for disposal at least annually and document approval. Cross-cut shred or use an approved confidential destruction service for paper. IT shall securely erase, cryptographically erase or physically destroy storage media according to its condition and sensitivity. Ordinary deletion, formatting or placing paper in general waste is insufficient for confidential records.

Record the record category, period covered, disposal authority, method, date, responsible person and confirmation. A supplier’s destruction certificate shall be retained with the disposal record. Reuse or sale of equipment requires verified removal of University information.

10.4 Backups and restoration

Backups are for recovery, not indefinite archives. IT shall document backup rotation and expiry. Information removed from live systems may remain in protected backups until the rotation expires; it shall not be reused for routine processing. Where selective deletion is not technically feasible, restrict access and record the expiry. After restoration, reapply valid deletion instructions and access restrictions before ordinary use resumes.

10.5 Record transfer and continuity

A department closing, changing systems or transferring responsibility shall inventory records, assign a receiving owner and document secure transfer. Student awards and other permanent records shall remain readable and accessible through planned format migration, integrity checks and controlled archival storage.

11 Assurance training and implementation

11.1 Privacy review before change

Complete Appendix D before a new or substantially changed collection, system, supplier or research use. A detailed impact assessment is mandatory for sensitive information at scale, biometrics, monitoring, automated significant decisions or a material reidentification risk. Document necessity, alternatives, risks, safeguards and residual risk. The President shall decide whether to authorise a high residual risk after receiving the lead's advice. An unlawful activity cannot be authorised as an exception.

11.2 Training and acceptable use

HR and the designated lead shall provide privacy induction before staff receive independent access to sensitive records and general induction within the first month. All authorised users shall complete annual refresher training and a confidentiality acknowledgement. Data owners, IT administrators and counselling or clinical personnel shall receive additional training appropriate to their access.

11.3 Monitoring and accountability

The designated lead shall report quarterly to the President on incidents, requests, overdue actions, access reviews, training, retention and high-risk projects. QA shall carry out an annual sample-based review using redacted evidence. Findings shall have owners, deadlines and verified closure. Publication of this policy does not substitute for these records.

Targets are 100 percent completion of scheduled access reviews, 100 percent training completion among active authorised users, and no overdue high-risk corrective actions without an approved escalation. Review performance against the request and incident targets in sections 8 and 9. Investigate missed targets and repeat issues.

11.4 Exceptions and noncompliance

Any exception shall record the affected control, justification, risk, compensating safeguards, approving authority and expiry. The lead shall review exceptions at least quarterly. Suspected misconduct shall be handled fairly under the applicable student, employment or contractual procedure. The University may restrict access immediately to contain a risk without prejudging disciplinary findings.

11.5 Implementation on approval

Deadline from approval	Required action
Immediately	Activate reporting route, prohibit unauthorised disclosure and preserve affected records.
Within 30 days	Confirm lead and unit contacts; publish notices; inventory priority records and systems; verify legal retention requirements.
Within 60 days	Complete priority access reviews, confidentiality acknowledgements, training and supplier risk checks.
Within 90 days	Test incident response and restoration; review sample requests and disposal controls; close or escalate gaps.

Appendix A Student privacy notice

For applicants current students and alumni

Knowledge University, Erbil, Kurdistan Region of Iraq, is responsible for the student information it handles. This notice describes the University's institutional commitments under KNU DP 01. A service-specific notice will explain additional uses where needed.

Information and purposes

We collect information needed for applications, identity and eligibility checks, registration, attendance, teaching, assessment, awards, fees, placements, student support and university administration. This may include contact and identity details, previous education, enrolment and results, financial transactions, communications and relevant system or security records. We collect health, disability, counselling or disciplinary information only where needed for an authorised purpose and with additional safeguards.

Sources and justification

Information comes mainly from you and your use of University services. It may also come from previous institutions, authorised representatives, examination or placement partners and competent authorities. We use information for education and service arrangements, applicable obligations, justified institutional functions or safety needs. We seek separate consent for optional uses where appropriate, such as featured promotional material. Required and optional fields will be identified when information is collected.

Access and sharing

Authorised staff receive access according to their duties. Relevant information may be shared with competent Ministries or authorities, payment and service providers, placement or academic partners, and authorised quality reviewers where necessary and justified. We verify requests and minimise what is shared. Overseas access or hosting requires prior review and appropriate safeguards. Family members, sponsors and employers do not automatically receive access to your records.

Retention and protection

We retain the official academic and award record for long-term verification. Other records follow the approved retention schedule, subject to binding requirements and legal holds. We use role-based access, secure storage and other proportionate safeguards. You may request information about a particular category's retention period and any relevant recipient or transfer arrangement.

Your choices requests and complaints

You may request access or correction, ask about processing, withdraw consent for optional uses, or seek deletion or restriction where appropriate. Required records may need to be retained. Contact the Directorate of Quality Assurance and Accreditation through Student Registration or the Presidency office. Registry: +964 750 3000 600 / +964 750 3000 700. Presidency: +964 750 3000 800. Ask for confidential routing; do not send sensitive documents to an unverified contact.

We aim to acknowledge requests within five working days and provide a substantive response within 30 calendar days, subject to applicable requirements and explained complexity. Complaints may be escalated to the President. Academic appeals follow their separate procedure. Material changes to this notice will be communicated through relevant University channels.

Appendix B Employee privacy notice

For job applicants academic and administrative personnel

Knowledge University, Erbil, Kurdistan Region of Iraq, is responsible for the personal information it handles for recruitment and employment. This notice covers permanent, temporary, visiting and part-time personnel, and other individuals working for the University where relevant.

Information and purposes

We process identity and contact details, qualifications, experience, references, appointment and contract details, attendance and leave, payroll and payment information, performance and development records, relevant disciplinary records, and necessary account or security logs. We use this information for recruitment, eligibility checks, work allocation, employment administration, payment, development, safety and authorised institutional reporting.

Health, disability and other sensitive records are restricted to those who need them. A manager will normally receive only the fitness, adjustment or absence information necessary for work arrangements. Detailed medical information is not placed in routine teaching or departmental files.

Sources and justification

Information normally comes from you, your work activities and authorised university records. Where appropriate it comes from referees, previous employers, qualification providers, service providers or competent authorities. Processing must be justified by employment arrangements, applicable obligations, authorised institutional functions, safety needs or appropriate consent for optional uses. Recruitment forms shall identify required fields and explain relevant checks.

Access sharing and professional profiles

HR, authorised managers, Finance and IT access information according to their duties. Relevant data may be shared with payment providers, competent authorities, approved service providers and authorised external reviewers where necessary. Professional staff profiles may contain approved work information; private contact details and identifiers shall not be published. Optional photographs and promotional testimonials require an appropriate permission or other recorded justification.

Retention security and monitoring

Personnel, recruitment and payroll information follows Appendix C and any overriding binding requirement or legal hold. Approved security and attendance monitoring must be proportionate and explained. Access is restricted and reviewed. Overseas access, external hosting and supplier arrangements require risk assessment and safeguards. Staff leaving the University must return records and devices and must not retain unauthorised copies.

Requests and complaints

You may request access, correction, information about processing, or deletion or restriction where appropriate, and withdraw consent for optional uses. Send requests to the Directorate of Quality Assurance and Accreditation through HR or the Presidency office. Presidency: +964 750 3000 800. This public telephone is a routing contact, not a dedicated confidential incident hotline.

The University aims to acknowledge within five working days and provide a substantive response within 30 calendar days. A refusal or delay will be explained. Complaints can be escalated to the President for independent review. Employment grievances and academic performance appeals retain their separate routes. No person shall face retaliation for raising a privacy concern in good faith.

Appendix C Retention schedule

Internal defaults for adoption

Apply these periods only after the owner checks for a longer binding requirement or an active hold. Periods are University policy defaults, not statements of Iraqi or KRG statutory law. Record any different authorised period, its source and review date in the compliance register. Keep the minimum authoritative record.

Record category and owner	Trigger and default period	Final action
Official enrolment final results award and transcript record Student Registration	Permanent minimum academic record; review integrity annually	Controlled archive
Unsuccessful student applications Registration	2 years after admission cycle closes	Secure deletion
Routine student administration and correspondence Registration or department	6 years after completion or withdrawal	Secure deletion
Examination scripts coursework and marking evidence Department	2 years after final result and closure of appeal, whichever is later	Delete; retain minimum final result
Personnel core employment file HR	7 years after employment ends	Review and securely delete
Unsuccessful recruitment applications HR	1 year after recruitment closes	Delete unless separate talent-pool agreement
Payroll fees tax and financial transactions Finance	7 years after relevant financial year closes	Review binding obligations then delete
Health counselling and disability case files Responsible service	7 years after last service contact; minor-related files require specific legal review before disposal	Restricted review and deletion
Complaints disciplinary cases and appeals Responsible owner	6 years after final resolution	Delete subject to hold
Research data and participant documentation Principal investigator	5 years after project closure or final publication, whichever is later; longer sponsor or ethics terms prevail	Anonymise or delete under plan
CCTV recordings Security and IT	30 days after recording unless incident preservation is needed	Automatic secure overwrite
Security and access logs IT	12 months after event; longer only for documented investigation	Secure deletion
Requests incidents risk and disposal evidence Designated lead	6 years after closure or supersession	Secure deletion
Routine backup sets IT	90 day rolling cycle unless a recorded recovery design needs a different period	Expire securely; no indefinite copies

Legal holds override every disposal date. Temporary working copies shall be deleted when their purpose ends. Consent records shall be kept while the use continues and for the period needed to demonstrate the related decision or resolve a claim.

Appendix D Data inventory and risk assessment

D1 Required inventory record

Each data owner shall complete one record per processing activity and update it after material changes. The examples below identify activity categories; actual storage locations, suppliers and access lists must be verified locally.

Activity	Accountable owner	Expected classification
Admissions registration and awards	Student Registration	Confidential
Recruitment employment and payroll	HR and Finance for their record sets	Confidential or Restricted
Assessment course files and student feedback	Department and QA for their record sets	Confidential
Counselling health and disability support	Responsible service head	Restricted
Research participant data	Principal investigator	Confidential or Restricted
Website forms public profiles and activity records	Website or service owner	Public approved output; restricted submissions
CCTV and account security records	Security and IT for their record sets	Confidential

Inventory reference _____ Activity _____ Owner and reviewer _____
Purpose and processing justification _____
People and data categories _____
Sources and notice location _____
Actual systems physical locations and hosting countries _____
Authorised roles and access approval reference _____
Recipients suppliers subcontractors and transfer safeguards _____
Retention trigger period disposal method and binding source _____
Security controls backup design and evidence references _____
Last review date _____ Next review date _____ Approval _____

D2 Risk and change assessment record

Project and sponsor _____ Assessment date _____
Necessity alternatives and expected benefit _____
Sensitive data minors monitoring AI or international access involved _____
Potential harms and affected people _____
Likelihood and impact before controls _____
Safeguards control owners and completion dates _____
Residual risk and consultation findings _____
Lead advice _____ President decision _____
Approval conditions review trigger and next review date _____

Classifications: Public means approved for release; Internal means operational nonpublic information; Confidential means personal or restricted business information; Restricted means highly sensitive information needing named or tightly limited access. Apply the highest relevant classification to mixed records.

Appendix E Access and confidentiality forms

E1 Access authorisation and removal

Request reference _____ Date _____
User name and staff number _____
Role department and line manager _____
Request type Grant / Change / Remove / Temporary access
System or paper record set _____
Minimum permissions and purpose _____
Sensitive or privileged access involved _____
Start date and time _____ End or expiry _____
Data owner approval _____ IT implementation _____
Training and confidentiality acknowledgement verified by _____
MFA or compensating safeguard verified _____
Access tested and implementation date _____
For departure or role change removal deadline _____
Removal confirmation and retained business record owner _____
Review date and reviewer _____

E2 Confidentiality acknowledgement

I acknowledge that personal and confidential information obtained through my University duties may be used only for authorised work. I will access only the records required for my role, keep my credentials private, verify recipients, use approved systems and protect paper records and devices.

I will not disclose student marks, personnel information, health or counselling details, research participant information or other confidential material without authority. I will not retain unauthorised copies, use personal channels for restricted records or submit personal data to unapproved AI tools. I will report suspected incidents immediately and cooperate with appropriate investigation and preservation requirements.

I will return University records and equipment when requested and on leaving. My confidentiality responsibilities continue after my role ends. This acknowledgement does not prevent lawful reporting, protected disclosures or cooperation with a competent authority. I understand that breaches may be addressed under applicable University procedures.

Name _____ Role and unit _____
Policy version received _____ Training date _____
Signature _____ Date _____
Manager or issuing officer _____ Date _____

E3 Periodic review evidence

Reviewer _____ Record or system _____
Review period _____ Permissions checked _____
Unnecessary access removed and date _____
Exceptions owner and expiry _____
Next review _____ Closure confirmed by _____

Appendix F Request and incident forms

F1 Individual information request

Form use is optional. Staff must also accept a clear request submitted in another format.

Case reference _____ Receipt date _____
Name and preferred secure contact _____
Relationship Student / Applicant / Employee / Former member / Other
Request Access / Copy / Correction / Deletion / Restriction / Complaint / Other
Records dates and details sought _____
Identity verification method and date _____
Representative authority verified if applicable _____
Acknowledgement date _____ Target response date _____
Owners asked to search and search outcome _____
Decision redactions or applicable restriction _____
Secure response method and dispatch date _____
Review route explained _____ Closure officer and date _____

F2 Data incident report and decision record

Report immediately; do not wait to complete this form. Keep detailed identifiers in a restricted attachment where necessary.

Incident reference _____ Reporter and contact _____
Occurrence date if known _____ Awareness date and time _____
Reported to IT and lead at _____ Location or system _____
What happened and current exposure _____
Data categories and estimated people and records affected _____
Sensitive data or safety risks _____
Containment actions owner and times _____
Evidence preserved and restricted location _____
Likely harm likelihood severity and remaining risk _____
President escalation date and initial assessment completed _____
Applicable notification duties deadlines and advice obtained _____
Notification or non-notification decision grounds and approving officer _____
Recipients notification content and dates _____
Recovery integrity checks and owner confirmation _____
Corrective actions owners and due dates _____
Lessons review date _____ Closure approval _____ Follow-up _____

Registers shall show reference, receipt or awareness date, owner, target, current status, outcome and closure date. Store detailed case records separately from general management reports.

Appendix G Adoption evidence and references

G1 Approval and implementation checklist

Record actual completion dates and evidence locations. An empty field indicates an action to complete, not compliance. Retain supporting evidence in the restricted A.10 accreditation folder.

Action and evidence	Accountable lead	Completed or reference
Authorised adoption and legal applicability check	President	
Lead and unit contacts confirmed; secure routing tested	President and QA	
Student and employee notices published and distributed	Registration HR and website owner	
Inventories and actual supplier or hosting register completed	Unit owners and IT	
Access sample reviewed and leaver removal demonstrated	IT HR and owners	
Retention defaults checked against binding requirements	Owners and designated lead	
Training delivered and acknowledgements obtained	HR and designated lead	
Backup restoration and incident exercise recorded	IT and designated lead	
Requests incidents and disposal registers activated	Designated lead and owners	
Quarterly report and annual assurance review scheduled	QA and President	

G2 Sources and relationship to existing documents

University information and contact routes were checked on 10 November 2026. The website supports institutional context, QA ownership, ERP access and relevant service areas. This policy's assignments, controls, retention defaults and targets are proposed institutional rules for adoption; the website does not establish that these controls already operate.

Knowledge University website and service navigation — https://knu.edu.iq/

Quality Assurance Office remit and published contact numbers — https://knu.edu.iq/tqa_message

University organisational structure — https://knu.edu.iq/knu_structure

Staff handbook reference — https://knu.edu.iq/handbook_staff

Location and contact — https://knu.edu.iq/location

ASIC University Standards of Accreditation Version 2.0 April 2023 — A.10.1 page 6; confirm the version issued for the current renewal. https://www.asic.org.uk/uploads/resources/Universities-SoA-V2.0-0423_2023-04-24-144102.pdf

Iraqi Constitution Article 17 — Supreme Judicial Council official text. https://www.sjc.iq/view.77/

Read alongside the current staff and student handbooks, academic ethics and professional conduct requirements, assessment and examination policy, course file requirements, and relevant employment, research and IT procedures. Resolve conflicts through the President and designated lead; binding law takes precedence.