CONFIDENTIALITY AND DATA PROTECTION POLICY

Jeryk EC Sdn. Bhd.
17-02, Q Sentral, 2A, Jalan Stesen
Sentral 2, Kuala Lumpur Sentral,
50470 Kuala Lumpur, Malaysia
202201020263 (1465960X)

TABLE OF CONTENTS

Jeryk EC Sdn. Bhd.
17-02, Q Sentral, 2A, Jalan Stesen
Sentral 2, Kuala Lumpur Sentral,
50470 Kuala Lumpur, Malaysia
202201020263 (1465960X)

Confidentiality and Data Protection Policy

1. Introduction

Jeryk EC is fully committed to safeguarding the personal data and privacy of all students, staff, and stakeholders. This Confidentiality and Data Protection Policy outlines how personal data is collected, used, stored, shared, and protected in a lawful, fair, and transparent manner.

The policy is designed to ensure compliance with the UK Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), and applicable local data protection regulations. It also reflects Jeryk EC's commitment to ethical data handling, institutional accountability, and best practices in academic governance.

2. Scope

This Confidentiality and Data Protection Policy applies to all personal data collected, processed, stored, shared, or otherwise handled by Jeryk EC, whether in electronic, digital, paper-based, or verbal form, and regardless of where or how the data is processed.

2.1 The policy covers personal data relating to, but not limited to:

- Students and prospective students, including applicants, enrolled learners, graduates, and alumni
- Employees and contracted staff, including academic staff, administrative staff, trainers, assessors, and consultants
- External stakeholders, including partners, awarding bodies, regulators, suppliers, agents, and visitors
- Any individual whose personal data is obtained through Jeryk EC's operations, services, or communications

2.2 This policy applies to all activities undertaken by Jeryk EC, including but not limited to:

- Student admissions, enrolment, assessment, certification, and progression
- Academic delivery, assessment management, quality assurance, and awarding body reporting
- Staff recruitment, employment administration, and professional development
- Use of learning management systems (LMS), digital platforms, websites, and communication tools
- Compliance with legal, regulatory, and contractual obligations

The policy applies to all Jeryk EC staff, contractors, volunteers, and authorized representatives who handle or have access to personal data as part of their roles. All such individuals are required to comply with this policy and any related data protection procedures, guidelines, or codes of conduct.

2.3 Third-Party Processing

a) This policy also extends to third-party service providers and partners who process personal data on behalf of Jeryk EC, including but not limited to:

- Awarding bodies and examination boards
- Learning management system providers
- IT service providers and cloud storage services
- External auditors, regulators, and professional advisers

b) International Data Transfers

Where personal data is transferred to recipients outside the country of origin, Jeryk EC ensures appropriate safeguards are in place to protect the data. These safeguards may include:

- Data transfer agreements incorporating GDPR-standard clauses
- Encryption and secure data transmission protocols
- Verification that international recipients maintain equivalent data protection standards

Jeryk EC ensures that all third parties engaged in data processing activities are subject to appropriate data protection agreements and are required to implement security measures that meet or exceed Jeryk EC's data protection standards.

2.4 Exclusions

This policy does not apply to information that has been fully anonymized and cannot be used to identify an individual. It also does not cover personal data processed independently by third parties where Jeryk EC does not act as the data controller.

2.5 Compliance with Local Data Protection Law

Jeryk EC ensures that all data processing activities comply not only with the UK GDPR and Data Protection Act 2018, but also with applicable local data protection laws where the institution operates, such as the Singapore Personal Data Protection Act (PDPA). All staff and third-party processors are required to adhere to these legal requirements.

3. Data Collection and Purpose

Jeryk EC collects only personal data that is necessary, relevant, and proportionate for its operations.

3.1 Categories of Data Collected

Student Information may include:

- Full name, contact details, and identification documents
- Academic records, assessment results, attendance records, and progression data
- Enrolment, payment, and certification information

Staff Information may include:

- Personal contact details
- Employment contracts, job roles, and performance records
- Payroll and statutory employment information

Other Stakeholder Information may include:

- Contact and communication details
- Records of correspondence or contractual arrangements

3.2 Purpose of Data Collection

Personal data is collected and processed for purposes including, but not limited to:

- Student administration, enrolment, assessment, and certification
- Employment administration and human resource management
- Compliance with legal, regulatory, and awarding body requirements
- Communication regarding courses, academic matters, institutional updates, and events
- Quality assurance, audits, and internal reviews

Personal data will not be processed for purposes incompatible with those stated above.

3.3 Legal Basis for Processing Personal Data

Jeryk EC collects and processes personal data only when there is a lawful basis, which may include:

- Consent: Where individuals have given explicit consent for specific data processing activities
- Contractual necessity: To fulfil obligations under enrolment, employment, or service agreements
- Legal obligation: To comply with statutory, regulatory, or accreditation requirements
- Legitimate interests: Where processing is necessary for Jeryk EC's legitimate interests, provided these do not override the rights of the individual

4. Rights of Individuals

In accordance with data protection legislation, individuals whose data is held by Jeryk EC have the following rights:

4.1 Right of access

Individuals have the right to request confirmation as to whether Jeryk EC holds personal data about them and, where applicable, to obtain access to such data. This includes:

- The categories of personal data held
- The purposes for which the data is processed
- The recipients or categories of recipients with whom the data has been shared
- The expected retention period or criteria used to determine retention

4.2 Right to rectification

Individuals have the right to request the correction or completion of personal data that is inaccurate, outdated, or incomplete. Jeryk EC will take reasonable steps to verify the accuracy of the data and update records promptly to ensure data integrity.

4.3 Right to object to processing circumstances

Individuals may object to the processing of their personal data where:

- Processing is based on legitimate interests
- Data is used for direct marketing purposes
- Processing is carried out for reasons that significantly affect the individual

Jeryk EC will review such objections carefully and cease processing unless there are compelling legitimate grounds or legal obligations requiring continuation.

4.4 Right to withdraw consent

Where the processing of personal data is based on the individual's consent, consent may be withdrawn at any time without penalty. Withdrawal of consent will not affect the lawfulness of processing carried out prior to the withdrawal. However, withdrawal may impact Jeryk EC's ability to provide certain services or academic functions where data processing is essential.

4.5 Right to restriction of processing

Individuals have the right to request the restriction of processing of their personal data in certain circumstances, including where:

- The accuracy of the data is contested
- Processing is considered unlawful
- The data is no longer required by Jeryk EC but is needed by the individual for legal claims

During periods of restriction, personal data will be stored securely and processed only with the individual's consent or where legally required.

4.6 Right to Erasure

Where permitted by law, individuals may request the deletion or anonymization of their personal data. This right is not absolute and may be limited where Jeryk EC is required to retain data to comply with:

- Legal or regulatory obligations
- Awarding body or accreditation requirements
- Academic record-keeping and certification standards

4.7 Exercising Data Protection Rights

All requests relating to data protection rights must:

- Be submitted in writing (via email or official request form)
- Include sufficient information to verify the requester's identity
- Clearly state the specific right being exercised

Jeryk EC will respond to all valid requests within statutory timeframes, typically within one calendar month, unless an extension is permitted under law. Where a request is complex or cannot be fulfilled, individuals will be informed of the reasons in writing.

4.8 Raising Data Protection Concerns or Complaints

Individuals may raise concerns or lodge complaints regarding the processing of their personal data by:

- Submitting a written request to the Data Protection Officer (DPO) via email or official form
- Clearly describing the concern or alleged breach of data protection requirements
- Providing sufficient information to allow verification of identity and investigation

Jeryk EC will respond to all valid complaints promptly, in accordance with statutory timelines, and will take appropriate corrective action where necessary.

5. Data Protection and Security

Jeryk EC implements robust organisational and technical measures to protect personal data from unauthorised access, disclosure, alteration, or loss.

These measures include:

- Access to personal data restricted strictly to authorised personnel on a need-to-know basis
- Mandatory confidentiality obligations and agreements for all staff and relevant third parties
- Secure storage of physical records and password-protected electronic systems
- Use of appropriate technical safeguards such as encryption, access controls, and secure backups
- Regular review of data protection practices and staff awareness training

All staff are responsible for complying with this policy and for safeguarding personal data in their care.

6. Data Breach Management

Jeryk EC takes the security and integrity of personal data seriously and has established robust procedures to respond to any suspected or actual data breaches promptly and effectively.

6.1 Reporting Breaches

- All staff, contractors, and relevant third parties must report any suspected or confirmed data breach immediately to Top Management or the designated Data Protection Officer (DPO).
- Reports should include all known details, such as the nature of the breach, affected systems or records, and the individuals potentially impacted.

6.2 Investigation and Assessment

- Jeryk EC will investigate all reported breaches promptly to determine the cause, scope, and potential impact on individuals and the institution.
- Investigations may involve reviewing access logs, interviewing staff, assessing technical vulnerabilities, and evaluating affected data types.

6.3 Corrective and Preventive Actions

- Once a breach is confirmed, appropriate corrective actions will be implemented immediately to mitigate risks and prevent further impact.
- Preventive measures may include system upgrades, enhanced access controls, staff retraining, policy revisions, or security audits.

6.4 Notification

- Where required by law or regulation, relevant authorities (e.g., Information Commissioner's Office in the UK) and affected individuals will be notified within prescribed timelines (typically within 72 hours of becoming aware of the breach).
- Notifications will provide clear information on the nature of the breach, potential impact, and any steps individuals should take to protect themselves.

6.5 Documentation and Accountability

- All breaches, investigations, actions taken, and communications are fully documented to ensure accountability and regulatory compliance.
- Documentation serves as evidence for internal audits, regulatory inspections, and continual improvement of data protection practices.

6.6 Data Protection Officer (DPO) Responsibilities

Jeryk EC has appointed a Data Protection Officer (DPO) responsible for:

- Monitoring compliance with data protection laws and internal policies
- Serving as the primary point of contact for data protection inquiries and complaints
- Advising on data protection impact assessments and best practices
- Coordinating responses to data breaches and liaising with relevant authorities

7. Data Retention

Jeryk EC retains personal data only for as long as necessary to fulfil operational, academic, legal, and regulatory obligations.

7.1 Retention Periods

- Student Records: Academic, enrolment, assessment, and certification records are retained for a minimum of six (6) years, or longer if required by awarding bodies, accreditation agencies, or statutory obligations.
- Staff Records: Employment, payroll, and performance records are retained for a minimum of six (6) years, or longer if legally required.
- Other Stakeholder Data: Contact, correspondence, and contractual records are retained for periods appropriate to their purpose.

7.2 Secure Disposal

- Once retention periods expire, personal data is securely destroyed, anonymized, or permanently deleted to prevent identification or misuse.
- Physical records are shredded or incinerated, and electronic data is deleted in accordance with industry-standard security practices.

7.3 Periodic Review

- Jeryk EC conducts periodic reviews of data retention schedules to ensure ongoing compliance with laws, regulatory requirements, and institutional policies.
- Reviews may adjust retention periods, update disposal methods, or revise classification of data based on operational needs or legal changes.

8. Policy Review

This Confidentiality and Data Protection Policy is reviewed periodically to ensure ongoing compliance with legal requirements and best practices in data governance. Any updates or amendments will be approved by the appropriate authority and communicated to stakeholders via official communication channels and the Jeryk EC website.

8.1 Frequency of Review

The policy is reviewed at least annually, or more frequently if required by changes in legislation, regulations, or institutional processes.

8.2 Communication of Updates

- Any updates or amendments to the policy are communicated to all stakeholders through official communication channels, including emails, intranet notices, and publication on the Jeryk EC website.
- Stakeholders are encouraged to review the latest version of the policy regularly and contact Jeryk EC with any questions or clarifications regarding its provisions.

8.3 Continuous Improvement

Feedback from staff, students, and external audits is used to continuously improve data protection measures, enhance awareness, and ensure that the institution maintains best practices in confidentiality and personal data management.

Stakeholders are encouraged to familiarize themselves with this policy and contact Jeryk EC for clarification where necessary.