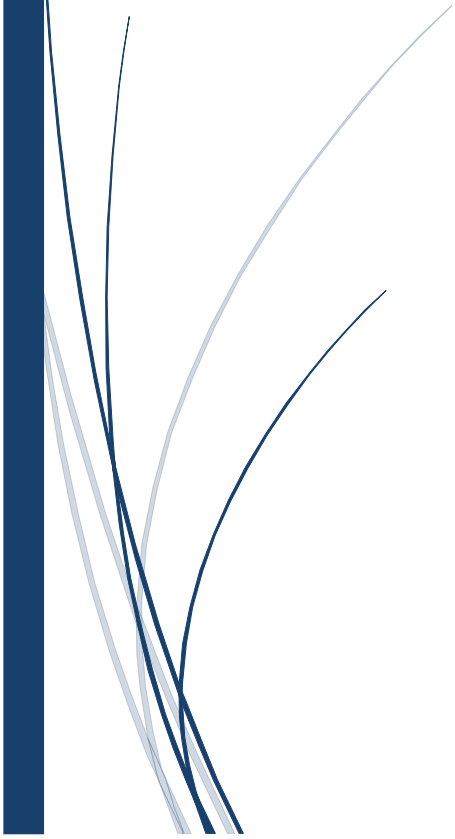
Kush Digital College (KDC) Data Protection Policy

Kush Digital College



Quality Assurance & Development Department
Kush digital college

Kush Digital College (KDC) Data Protection Policy

Document Title	**KDC Data Protection Policy**
Scope (applies to)	All staff, students, alumni, contractors, and third-party service providers handling personal data on behalf of KDC.
Document author and School	Legal and Compliance Department, or Information Governance Department.
Section responsible for policy maintenance & review	Data protection section/ information security
Approving body	Data Protection and Compliance Committee (Ref: [Committee Name & Minute Reference])
Date of approval	
Review date/ Expiry Date	
Date of effect/ Approved Date	
Information Classification	Internal and External Use
Public access online	YES
Public access on request by mail	YES
Version	1.0
Key Terms	Personal Data, Data Subject, Data Controller, Data Processor, Data Protection Impact Assessment (DPIA), Consent, GDPR, Data Breach, Encryption
Reference of this policy	General Data Protection Regulation (GDPR)
The latest version of this document to be found at:	Kdc.edu.uk/policy-1

1. Policy Title: KDC Data Protection Policy

2. Purpose and Scope

2.1 Purpose:

Kush Digital College (KDC) is committed to safeguarding the privacy and security of personal data in accordance with the **General Data Protection Regulation (GDPR)** and the **UK Data Protection Act 2018**. As an online educational institution, KDC processes personal data lawfully, transparently, and securely, ensuring compliance with all relevant data protection regulations. This policy aims to protect the rights of individuals and ensure that personal data is managed with confidentiality and care.

2.2. Scope:

This policy applies to all personal data processed by KDC relating to students, staff, alumni, contractors, and third-party service providers. It governs data collected through KDC's digital platforms and operations, ensuring adherence to GDPR and the UK Data Protection Act 2018. The policy supports KDC's mission to deliver digital education while protecting the privacy rights of all individuals.

2.3. Policy Objectives:

1. **Ensure Data Security and Compliance**: Protect personal data through secure practices, supporting KDC's compliance with GDPR and other relevant regulations.
2. **Promote Transparency and Trust**: Foster a culture of transparency, where data subjects understand how their information is used and their rights are respected.
3. **Support Institutional Integrity**: Align data protection practices with KDC's commitment to ethical, responsible management of data and information.

2.4. Data Protection Principles

KDC's data protection practices are grounded in key principles that ensure all personal data is handled responsibly and transparently.

- **Data Minimisation**: Only the minimum necessary personal data is collected, stored, and processed to achieve KDC's educational objectives.

- **Accuracy**: KDC ensures that personal data remains accurate, complete, and up-to-date, with processes in place for prompt correction as necessary.
- **Accountability**: KDC takes responsibility for data protection and complies with GDPR standards, ensuring that all data handling activities are ethical and lawful.

3. DEFINITIONS

- **Personal Data**: Any information relating to an identifiable person who can be directly or indirectly identified.
- **Data Subject**: The individual to whom the personal data relates.
- **Data Controller**: KDC, which determines the purpose and means of processing personal data.
- **Data Processor**: Any third party that processes personal data on behalf of KDC.
- **Consent**: A clear affirmative action signifying agreement to the processing of personal data.
- **GDPR**: The General Data Protection Regulation, a law governing data protection and privacy in the EU and the UK.
- **Data Breach**: A security incident leading to accidental or unlawful access, loss, or disclosure of personal data.

4. KEY ROLES AND RESPONSIBILITIES

- **Data Protection Officer (DPO)**: Monitors compliance, conducts **Data Protection Impact Assessments (DPIAs)**, and serves as the contact point for data subjects and the **Information Commissioner's Office (ICO)**.
- **Heads of Departments**: Ensure compliance with data protection obligations within their teams and that personal data is processed according to KDC's procedures.
- **All Staff and Contractors**: Must follow the principles outlined in this policy and immediately report any suspected data breaches.

5. POLICY STANDARDS AND PROCEDURES

5.1. Data Collection and Processing

- Personal data must be collected and processed lawfully, fairly, and transparently.
- Data is collected only for specific, legitimate purposes and not further processed in a manner incompatible with these purposes.
- The amount of personal data collected is minimized to what is necessary for the intended purpose.

5.2. Lawful Basis for Processing

KDC processes personal data under the following lawful bases as per **Article 6 of GDPR**:

- **Consent**: Explicit consent obtained from the data subject.
- **Contractual Necessity**: Processing is necessary to fulfill contractual obligations.
- **Legal Obligation**: Processing required by law.
- **Legitimate Interests**: Processing based on KDC's legitimate interests, provided it does not override the data subject's rights.

5.3. Data Security

- Personal data is stored securely using encryption, restricted access, and secure IT systems.
- Data transfers are encrypted, and only authorized personnel have access to personal data.

5.4. Data Retention

- Personal data is retained only for as long as necessary to fulfil the purpose for which it was collected, in line with KDC's **Data Retention Policy**.
- Once the retention period has expired, data is securely deleted or anonymised.

5.5. Data Subject Rights

KDC ensures that data subjects can exercise the following rights under GDPR:

- **Right to Access**: Data subjects can request access to their personal data.
- **Right to Rectification**: Data subjects can request corrections to inaccurate or incomplete data.
- **Right to Erasure**: Data subjects can request the deletion of personal data (right to be forgotten).
- **Right to Restrict Processing**: Data subjects can request a restriction on the processing of their data.

- **Right to Data Portability**: Data subjects can request their personal data in a structured format to be transferred to another service.
- **Right to Object**: Data subjects can object to data processing based on legitimate interests or direct marketing.

5.6. Data Breach Management

- In case of a data breach, KDC will notify the ICO within 72 hours if the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Data subjects will be informed promptly if the breach poses a high risk to their rights.

5.7. Data Protection Impact Assessments (DPIAs)

- DPIAs are conducted for any new processing activities involving high-risk data processing to evaluate and mitigate risks to data subjects.

5.8. Third-Party Data Sharing and Due Diligence

KDC ensures that data shared with third-party vendors or partners complies with GDPR, safeguarding personal information during and after transfer.

- **Third-Party Data Sharing Policies**: Data sharing is governed by strict contracts that require third parties to adhere to GDPR standards and KDC's data security protocols.
- **Vendor Compliance and Risk Assessment**: KDC conducts regular risk assessments of vendors to ensure ongoing compliance, including annual evaluations and due diligence checks.

5.8. Consent Management and Record-Keeping

KDC manages and records consent processes to ensure transparency and compliance with GDPR's lawful basis requirements.

- **Consent Management Process**: Consent is obtained in a clear, affirmative manner, with records kept of when, how, and for what purpose consent was given.
- **Documenting Lawful Basis for Processing**: KDC records the lawful basis for each processing activity (e.g., consent, legitimate interests), ensuring documentation is readily available for audits or reviews.

5.9. Specific Guidelines for Data Retention and Disposal

KDC adheres to structured data retention and disposal guidelines to prevent unnecessary retention of personal information and ensure secure disposal.

- **Retention Schedules for Data Types**: Data retention periods are specified for each data type, such as student records, staff information, and vendor data, with periodic reviews for compliance.
- **Data Disposal Procedures**: Data is securely deleted or anonymised upon expiry of the retention period, using secure disposal methods to prevent unauthorised access.

5.10. Detailed Data Breach Management Procedures

KDC has established a structured process for responding to data breaches, ensuring quick and effective containment and reporting.

- **Steps for Data Breach Response**: A detailed breach response includes initial containment, risk assessment, notification to affected individuals, and reporting to the regulatory authority within 72 hours if required.
- **Post-Breach Review and Reporting**: After a breach, a review is conducted to assess the cause and improve security measures, with findings documented to prevent recurrence.

5.11. Regular Data Protection Training and Awareness

KDC provides regular training on data protection for all staff and stakeholders to promote compliance and awareness.

- **Mandatory Training Programs**: All staff and contractors complete data protection training, covering secure data handling, GDPR basics, and incident reporting, with periodic refreshers.
- **Ongoing Awareness Campaigns**: Awareness campaigns reinforce data protection practices, emphasising the importance of compliance and updating staff on policy changes.

6. FORMS/INSTRUCTIONS/RELATED DOCUMENTS

- **Data Subject Request Form**: For individuals to request access, correction, or deletion of their personal data.
- **Data Breach Incident Report Template**: To document and report data breaches.

- **KDC Data Retention Policy**: Provides guidelines for retaining and securely disposing of personal data.
- **Data Retention Schedule**

7. Related Policies and Documents

- Continuous Improvement Policy
- Program and Curriculum Review Policy
- Student Services and Support Policy

8. Approval and Revision History

- Approval Date: [Insert Date]
- Approved By: KDC Governing Board
- Next Review Date: [Insert Date]
- Revision History: [Insert details of any policy changes]

9. CONTACT INFORMATION

- **Data Protection Officer (DPO)**: For any queries or concerns regarding data protection, contact [Insert Contact Email].
- **IT Support Team**: For queries related to data security and technical assistance, contact [Insert IT Department Contact Email].

APPENDICES

Appendix A: Data Retention Schedule

Appendix B: Data Subject Rights Guide