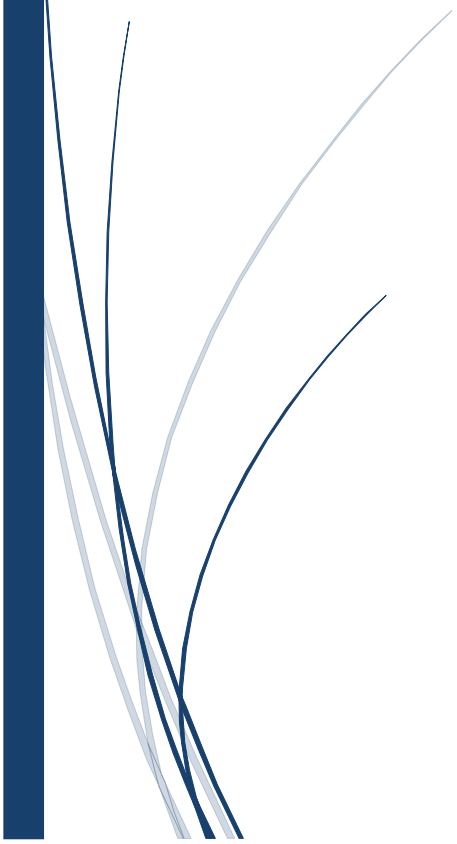
KDC Cybersecurity Policy

Kush Digital College



Quality Assurance & Development Department
Kush digital college

Document Title	**KDC Cybersecurity Policy**
Scope (applies to)	All staff, students, and third-party service providers using KDC's IT systems.
Document Author (Dept)	IT and Information Governance Department
Approving Body	Data Protection and Compliance Committee (Ref: [Committee Name & Minute Reference])
Date of Approval	[Insert Approval Date]
Date of Implementation	[Insert Implementation Date]
Responsibility for Implementation	IT Department, Cybersecurity Team
Date of Review	[Insert Review Date]
Date of Next Review	Every 3 years unless otherwise required
Information Classification	Internal and External Use
Public Access Online	YES
Public Access on Request by Mail	YES
Current Version Number	1.0
Key Terms	Firewalls, Secure Configuration, Malware Protection, Patch Management, Access Control
Latest Version Found at	kdc.edu.uk/policy-1

1. TITLE OF POLICY: KDC Cybersecurity Policy

2. PURPOSE AND SCOPE OF POLICY

The KDC Cybersecurity Policy establishes the standards and practices needed to protect KDC's digital environment from cyber threats. This policy defines cybersecurity measures necessary for safeguarding KDC's IT infrastructure, including protective measures for sensitive data, compliance with cybersecurity standards, and prevention of unauthorized access.

2.1 Purpose

To ensure KDC's IT systems and data are secure, resilient against cyber threats, and compliant with National Cyber Security Centre (NCSC) and Cyber Essentials standards.

2.2 Scope

This policy applies to all users of KDC's IT systems, including staff, students, and third-party service providers, and encompasses all aspects of cybersecurity from access control to patch management.

3. DEFINITIONS

- **Firewall:** A security system that monitors and controls incoming and outgoing network traffic based on security rules.
- **Patch Management:** The process of updating software and systems to address security vulnerabilities.
- **Access Control:** Mechanisms that ensure only authorized users can access specific IT systems and data.

4. POLICY STATEMENT

Kush Digital College (KDC) is dedicated to maintaining a secure IT environment to protect the institution's data, digital resources, and users from cyber threats. This policy ensures that all IT systems meet established cybersecurity standards, including robust protection against malware, secure configurations, and effective access control measures.

5. ROLES AND RESPONSIBILITIES

- **Cybersecurity Team:** Implements and manages all cybersecurity measures, including firewalls, malware protection, and patch management.

- **IT Department:** Ensures all systems are securely configured, regularly updated, and monitored for security compliance.
- **Staff and Students:** Required to follow the cybersecurity measures outlined in this policy and report any suspicious activities to the Cybersecurity Team.

6. POLICY STANDARDS AND PROCEDURES

- **Firewalls:** Firewalls are installed on all KDC networks, monitored, and configured to prevent unauthorized access.
- **Secure Configuration:** All systems and devices must be configured with strong passwords, secure settings, and regular reviews to maintain security.
- **Malware Protection:** Antivirus software is installed and regularly updated across all devices to protect against malware.
- **Patch Management:** Software and systems are updated regularly to fix vulnerabilities and maintain security compliance.
- **Access Control:** Access to IT systems and data is restricted based on the principle of least privilege, ensuring that only authorized personnel have access to sensitive information.

7. COMPLIANCE AND MONITORING

The Cybersecurity Team and IT Department conduct regular audits and monitoring to ensure compliance with this policy. Any non-compliance or security breaches are documented, investigated, and reported to the Data Protection and Compliance Committee.

8. APPEALS AND EXCEPTIONS

Requests for exceptions to this policy must be submitted to the Data Protection and Compliance Committee, along with a justification and any proposed risk mitigation measures.

9. REVIEW AND REVISION

This policy is reviewed every three years or as needed to address changes in cybersecurity standards or regulatory requirements. Updates are made to reflect evolving cybersecurity threats and technological advancements.

10. FORMS/INSTRUCTIONS/RELATED DOCUMENTS

- **Cyber Incident Report Form**
- **IT Security Guidelines Document**

11. CONTACT INFORMATION

For any cybersecurity concerns or incidents, please contact the Cybersecurity Team at cybersecurity@kdc.edu.uk.

12. REFERENCES AND RESOURCES

- **NCSC Cybersecurity Guidance**
- **Cyber Essentials Standards**
- **KDC Data Protection Policy**

13. APPENDICES

- **Appendix A:** Firewall Configuration Guidelines
- **Appendix B:** Malware Protection Standards

14. APPROVAL AND REVISION HISTORY

- **Approval Date:** [Insert Approval Date]
- **Approved By:** Data Protection and Compliance Committee
- **Next Review Date:** [Insert Review Date]
- **Revision History:** None; Initial Version