مدرسة الشعاع الهندية
للبنات والبنين
Radiant Indian School
For Girls & Boys

RADIANT INDIAN SCHOOL FOR GIRLS AND BOYS,SHARJAH

PASSWORD PROTECTION POLICY

Objective:

The Password Protection Policy aims to establish guidelines and best practices for creating, managing, and safeguarding passwords within the school's digital ecosystem. By implementing this policy, the school seeks to enhance cybersecurity resilience, protect sensitive information, and promote responsible password management among students, staff, and stakeholders.

1. Password Creation:

Complexity Requirements: All passwords must adhere to complexity requirements, including a minimum length of eight characters, a combination of uppercase and lowercase letters, numbers, and special characters.

Avoidance of Common Patterns: Users should refrain from using common patterns or easily guessable information (e.g., sequential numbers, birthdates, dictionary words) in their passwords.

Regular Updates: Users must regularly update their passwords to mitigate the risk of unauthorized access. Password changes should occur at least every six months or as mandated by the IT department.

2. Password Management:

Individual Account Responsibility: Each user is responsible for maintaining the confidentiality and security of their passwords. Sharing passwords or allowing unauthorized access to accounts is strictly prohibited.

Unique Passwords: Users should use unique passwords for each of their accounts to prevent unauthorized access in the event of a security breach.

Password Storage: Storing passwords in plaintext or insecure mediums (e.g., sticky notes, unencrypted files) is prohibited. Password managers, encrypted storage solutions, or secure memory techniques are recommended for storing passwords securely.

3. Access Control:

Role-based Access: Access to digital resources and systems should be granted based on the user's role and responsibilities within the school's hierarchy.

Least Privilege Principle: Users should be granted the minimum level of access necessary to perform their job functions effectively. Access privileges should be reviewed periodically and adjusted as needed.

4. Authentication Mechanisms:

Multi-Factor Authentication (MFA): Where feasible, MFA should be implemented to add an additional layer of security beyond passwords. This may include SMS codes, biometric authentication, or hardware tokens.

5. Incident Response:

Reporting Security Incidents: Users must promptly report any suspected security incidents, such as unauthorized access attempts or compromised passwords, to the IT department or designated security personnel.

Password Reset Procedures: In the event of a suspected or confirmed security incident involving passwords, affected users should follow the designated password reset procedures to regain control of their accounts.

6. Education and Awareness:

Training Programs: Regular training sessions and awareness programs should be conducted to educate users about the importance of password security, common threats (e.g., phishing, social engineering), and best practices for safeguarding passwords.

Policy Acknowledgment: All users must acknowledge their understanding and agreement to comply with the Password Protection Policy upon enrollment or employment at the school and periodically thereafter.

7. Policy Enforcement:

Compliance Monitoring: The computer department or designated personnel shall monitor compliance with the Password Protection Policy through periodic audits, access logs analysis, and security assessments.

Consequences of Non-Compliance: Non-compliance with the Password Protection Policy may result in disciplinary action, including but not limited to account suspension, loss of privileges, or termination of enrollment/employment.

Conclusion:

By adhering to the Password Protection Policy, the school can mitigate the risk of unauthorized access, data breaches, and other cybersecurity incidents. Additionally, promoting a culture of password security and accountability among students, staff, and stakeholders will contribute to a safer and more resilient digital environment within the school community.