TOWNLEY
EST 1937
GRAMMAR SCHOOL

CYBERSECURITY (EXAMS) POLICY

1. Purpose and Scope

This Cybersecurity Policy is established to ensure compliance with the Joint Council for Qualifications (JCQ) General Regulations. It aims to protect the integrity, confidentiality, and availability of data related to assessments, exams, and student information while maintaining robust measures to safeguard against unauthorised access and cyber threats. This policy applies to all individuals with access to exam-related data, including staff, students, external examiners, and third-party vendors.

2. Policy Objectives

- To protect the confidentiality, integrity, and availability of assessment and exam-related data
- To ensure all parties involved in exams and assessments comply with JCQ General Regulations regarding data protection and cybersecurity
- To mitigate risks related to unauthorised access, data breaches, and cyber-attacks that could compromise exam security or data privacy.

3. Cybersecurity Responsibilities

- Data Protection Officer (DPO): Responsible for overseeing the implementation of this policy and ensuring compliance with data protection laws and JCQ regulations
- IT Department: Ensures the technical security infrastructure is in place, including secure networks, systems, and backups
- Exams Manager: Responsible for ensuring cybersecurity measures are followed throughout the exam process, including secure transfer and storage of data
- Staff and Users: All staff with access to exam systems and data must adhere to the security protocols outlined in this policy, including strong password management, secure handling of exam data, and reporting any security incidents.

4. Access Control

- Authentication: All individuals accessing exam data must use secure authentication methods (e.g., two-factor authentication or strong passwords) to ensure that only authorised users can access sensitive information
- Role-Based Access Control (RBAC): Access to exam data is granted based on the user's role. Permissions are defined according to the job responsibilities, ensuring that staff members only have access to the data necessary for their tasks
- Regular Access Reviews: Access rights must be reviewed periodically to ensure that only authorised personnel have access to sensitive data. Immediate revocation of access is required when personnel leave or change roles.

5. Data Protection and Encryption

- Encryption of Data: Sensitive exam-related data (e.g., exam papers, student records) must be encrypted both in transit and at rest. All communication channels (e.g., email, file transfers) must be encrypted using industry-standard encryption protocols (e.g., TLS, AES)
- Data Storage: Exam data must be securely stored, using encrypted systems and storage devices. Physical access to storage devices should be restricted to authorised personnel only
- Retention and Disposal: Exam data must be retained only as long as necessary in compliance with JCQ regulations. Once data is no longer required, it must be securely deleted using appropriate data destruction methods.

6. Incident Response and Reporting

- Incident Reporting: All staff must report any suspected or actual cybersecurity incidents immediately to the IT Department and the Exams Officer. This includes unauthorised access, data breaches, system malfunctions, or potential cyber-attacks
- Incident Response Plan: An incident response plan should be in place to address and resolve any cybersecurity incidents promptly. The plan should include steps for containment, investigation, communication, and recovery
- Regular Drills: Regular drills must be conducted to test the effectiveness of the incident response plan and ensure all staff are familiar with reporting and response procedures.

7. Secure Handling of Exam Papers and Results

- Physical Security: Printed exam papers must be stored in secure locations, with restricted access to authorised personnel only. Any physical copies of exam papers should be protected from unauthorised viewing or access
- Digital Security: Digital exam papers and results must be protected by strong security protocols, such as encryption and secure user access control
- Transfer of Exam Data: Any transfer of exam data (e.g., to exam boards or other authorised organisations) must be done using secure, encrypted methods to prevent interception or tampering.

8. Training and Awareness

- Staff Training: All staff involved in the exam process must receive regular cybersecurity training, particularly on data protection, phishing attacks, secure password management, and safe use of devices and networks
- Awareness Campaigns: Regular cybersecurity awareness campaigns should be conducted to ensure that staff remain informed of the latest threats and best practices
- Testing Knowledge: Periodic testing of staff knowledge on cybersecurity protocols and JCQ regulations should be conducted to ensure compliance.

9. Compliance with Legal and Regulatory Requirements

- JCQ Regulations: This policy is aligned with the JCQ General Regulations and adheres to their specific requirements regarding the security of exam papers, results, and data handling
- Data Protection Laws: The organisation must comply with all relevant data protection laws, including the UK Data Protection Act 2018, the GDPR, and other applicable regulations regarding personal data and student privacy.

10. Audit and Review

- Security Audits: Regular security audits must be conducted to assess the effectiveness of this policy and identify any vulnerabilities. Audits should include checks on access controls, data encryption, and incident response processes
- Policy Review: This cybersecurity policy should be reviewed annually or following significant changes in technology or regulations. Any changes to JCQ regulations or data protection laws must prompt an immediate review of the policy.

11. Disciplinary Actions

Any violation of this cybersecurity policy or failure to comply with JCQ regulations may result in disciplinary action. This may include revocation of access to exam data, suspension, or termination of employment, depending on the severity of the violation.

12. Conclusion

This Cybersecurity Policy is designed to ensure that the organisation upholds the highest standards of security for exam data, in full compliance with the JCQ General Regulations. By following these guidelines, the organisation will protect against potential cyber threats and maintain the integrity and confidentiality of exam processes.