CROWN PRIVATE SCHOOL مدرسة كراون الخاصة British Curriculum المنهاج البريطاني	CYBER SECURITY POLICY

PROCESS NAME:	Cyber security Policy	**CREATION DATE:**	10/09/2022
PROCESS MANAGER:	IT Administrator	**LAST REVISION:**	05/02/2025
PREPARED BY	Rajeesh Kumar – IT-Admin	**APPROVED BY**	Dr. Kishor Pillai- Principal
APPLIES TO:	All Staff All Parents All Children	**RELATED DOCUMENT(S):**	Acceptable Use policy Online safety policy Password Policy

1. Introduction The purpose of this Cybersecurity Policy is to establish guidelines and procedures to protect the school's IT systems, sensitive data, and digital resources from cybersecurity threats. This policy applies to all staff, students, contractors, and third-party vendors who access the school's network and information systems.

2. Scope This policy covers all IT infrastructure, including but not limited to:

- School networks and servers
- Email systems and cloud storage
- Workstations, laptops, and mobile devices
- Internet and Wi-Fi access
- Software applications and databases
- Third-party and cloud-based services

3. Cybersecurity Best Practices All users are expected to follow these best practices to ensure a secure IT environment:

- **Strong Passwords:** Use complex passwords and change them periodically.
- **Multi-Factor Authentication (MFA):** Enable MFA where applicable.
- **Phishing Awareness:** Be cautious of suspicious emails, links, and attachments.
- **Secure Browsing:** Avoid visiting untrusted websites and downloading unauthorized software.
- **Regular Software Updates:** Ensure operating systems, applications, and antivirus programs are up to date.
- **Device Security:** Lock devices when not in use and report lost or stolen devices immediately.
- **Data Protection:** Avoid storing sensitive data on personal devices or unsecured cloud services.

4. Network and System Security

- The IT department will enforce firewalls, intrusion detection systems, and endpoint security solutions to prevent unauthorized access.
- Wi-Fi access will be restricted and monitored to prevent unauthorized usage.
- Access to critical systems will be limited based on user roles and responsibilities.

5. Incident Response and Reporting

- Any suspected cybersecurity incidents, such as data breaches, malware infections, or unauthorized access, must be reported to the IT department immediately.
- The IT team will investigate, mitigate risks, and take corrective actions to prevent recurrence.

6. Backup and Disaster Recovery

- Regular backups of school data will be conducted and securely stored.
- A disaster recovery plan will be maintained to ensure business continuity in case of cyber incidents.

7. Compliance and Monitoring

- The IT department will conduct periodic security audits to ensure compliance with this policy.
- Users who violate cybersecurity policies may face disciplinary action, including access restrictions and legal consequences if necessary.

8. Policy Review This policy will be reviewed annually to ensure it remains up to date with evolving cybersecurity threats and best practices.

By adhering to this policy, all stakeholders contribute to a secure and resilient IT environment at the school.

-