CROWN PRIVATE SCHOOL
مدرسة كراون الخاصة
British Curriculum المنهاج البريطاني

REMOTE ACCESS POLICY

PROCESS NAME:	Remote Access 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	**RELATED DOCUMENT(S):**	Acceptable use Policy

1. Introduction

Crown Private School is committed to ensuring secure remote access to its IT systems and data. This policy establishes guidelines for remote access to protect the integrity, confidentiality, and availability of school resources while enabling employees, contractors, and other authorized personnel to work remotely.

2. Scope

This policy applies to all employees, contractors, vendors, and other personnel who require remote access to the school's IT systems, applications, or data.

3. Policy Statement

Remote access to Crown Private School's IT systems must be controlled and managed securely. Users must adhere to security best practices to prevent unauthorized access, data breaches, and cyber threats.

4. Access Control

- Remote access will be granted only to authorized users based on job requirements.
- All users must use strong authentication methods (e.g., multi-factor authentication, VPN access).
- Access will be monitored and reviewed periodically.
- User accounts with remote access privileges must be disabled when no longer required.

5. Security Requirements

- Only school-approved devices or secured personal devices with updated security software are allowed for remote access.
- End-to-end encryption must be used for all remote sessions.
- Users must not store sensitive school data on personal devices.
- All devices must have up-to-date antivirus and security patches installed.

6. Acceptable Use

- Remote access should be used strictly for work-related activities.
- Users must not share login credentials or allow unauthorized persons to access school systems.
- Accessing inappropriate or non-work-related websites while using school systems remotely is prohibited.

7. Network and Connection Security

- Remote access must be conducted through a secure VPN or other approved encrypted channels.
- Public Wi-Fi or unsecured networks must not be used for accessing school systems.
- Users must log off after completing remote work and ensure unattended devices are locked.

8. Incident Reporting

- Any suspected security incidents, breaches, or unauthorized access must be reported to the IT department immediately.
- Users must comply with the school's Incident Response Policy.

9. Compliance and Violations

- Any violations of this policy may result in disciplinary action, including revocation of remote access privileges.
- The IT department will conduct periodic audits to ensure compliance with this policy.

10. Policy Review This policy will be reviewed annually and updated as necessary to address emerging security threats and technological changes.