| CROWN PRIVATE SCHOOL<br>مدرسة كراون الخاصة<br>British Curriculum المنهاج البريطاني | # DISASTER RECOVERY POLICY |
|---|---|

|  |  |  |  |
|---|---|---|---|
| **PROCESS NAME:** | Disaster Recovery 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):** | Incident Response Policy |

## 1. Introduction

Crown Private School recognizes the critical importance of maintaining IT services and data integrity in the event of a disaster. This Disaster Recovery Policy establishes a framework for responding to and recovering from incidents that disrupt IT operations, ensuring continuity of educational and administrative activities.

## 2. Scope

This policy applies to all IT infrastructure, including servers, networks, applications, data storage, and communication systems used by Crown Private School. It covers natural disasters, cyber-attacks, hardware failures, data breaches, and other significant disruptions.

## 3. Objectives

- Minimize downtime and restore normal operations as quickly as possible.
- Protect sensitive school, student, and staff data from loss or unauthorized access.
- Ensure compliance with relevant data protection regulations, including GDPR.
- Establish clear roles and responsibilities for disaster recovery.

## 4. Disaster Recovery Team

The Disaster Recovery Team (DRT) will be responsible for executing the recovery plan. Key roles include:

- IT Manager: Oversees disaster recovery efforts.
- System Administrators: Handle server and network restoration.
- Data Protection Officer: Ensures compliance with data security policies.
- Communication Officer: Manages internal and external communications.

### 5. Risk Assessment & Business Impact Analysis (BIA)

- Identify potential threats (e.g., cyber-attacks, power failures, natural disasters).
- Assess the impact of system failures on school operations.
- Prioritize critical systems and define acceptable recovery time objectives (RTO) and recovery point objectives (RPO).

### 6. Backup & Data Protection

- All critical data must be backed up regularly (daily incremental and weekly full backups).
- Backups must be stored in secure, off-site locations.
- Backup integrity must be tested quarterly.

### 7. Disaster Recovery Plan (DRP)

- **Activation**: Criteria for declaring a disaster and activating the DRP.
- **Response Procedures**: Steps to contain the impact and prevent further damage.
- **Recovery Process**: Sequence for restoring critical IT services.
- **Post-Recovery Review**: Evaluation of the response and identification of improvements.

### 8. Communication Plan

- Internal notifications: Inform staff, students, and stakeholders.
- External notifications: Coordinate with service providers and regulatory bodies if required.
- Media and Public Relations: Designated personnel to handle external inquiries.

### 9. Testing & Training

- Annual disaster recovery drills must be conducted.
- Staff must be trained on their roles in the recovery process.
- Regular reviews and updates to the policy based on test results.

### 10. Policy Compliance & Review

- Non-compliance with this policy may result in disciplinary action.
- The IT department will review this policy annually and update it as necessary.

**11. Contact Information** For disaster recovery assistance, contact the IT Helpdesk