Policy for Handling a Server Crash in the School

Purpose

To establish a clear and efficient procedure for handling server crashes within the school network to minimize disruption to school operations and maintain data integrity.

Scope

This policy applies to all school staff, students, and IT personnel involved in the use of the school's digital systems and networks.

Policy Statement

In the event of a server crash, the following steps will be taken:

1. Immediate Response

- **Notification:** The IT department must be notified immediately by the staff or department affected by the server crash. A report can be submitted through email, phone, or in person.
- **Initial Assessment:** IT personnel will conduct a quick assessment to identify the cause of the crash and the affected areas (e.g., specific servers, databases, communication systems, or online learning platforms).

2. Communication

- **Internal Communication:** The IT department will inform the principal, vice-principals, and relevant department heads about the crash, including the scope of the issue and the estimated recovery time.
- **School-wide Notification:** A message will be sent to all staff, teachers, and students via email, messaging apps, or announcements about the issue, including temporary workarounds (if available) and updates on the expected resolution.

3. Recovery Process

- **Backups:** IT staff will immediately check recent backups to determine the latest recoverable version of the server data. Daily backups are essential to ensure minimal data loss.
- **System Reboot:** If the crash is deemed recoverable by a system reboot, IT staff will attempt to restart the server safely and monitor the system's performance for any recurring issues.
- **Advanced Recovery:** If the crash involves data corruption or hardware failure, the IT department will begin recovery from backups and, if necessary, replace or repair faulty hardware.

4. Temporary Solutions

- **Workarounds:** If certain essential services are disrupted (e.g., access to online platforms or attendance systems), the IT department will provide temporary alternatives or manual processes (such as offline attendance tracking or use of cloud-based alternatives) until full service is restored.
- **Priority Services:** The restoration of critical systems (such as school databases, grading systems, and email servers) will be prioritized to ensure minimal impact on school operations.

5. Monitoring and Testing

- After restoring the server, IT staff will closely monitor its performance for at least 24-48 hours to ensure stability.
- Functional testing will be conducted on all systems and databases to confirm they are working as expected.

6. Communication of Resolution

- **Notification:** Once the server is restored and functioning normally, a final update will be communicated to the school community, indicating that normal operations can resume.

7. Reporting and Documentation

- A detailed incident report will be prepared by the IT department, outlining the cause of the crash, the recovery steps taken, and preventive measures to avoid future occurrences.
- This report will be submitted to the principal's office for review and kept on record for future reference.

8. Preventive Measures

- Regular maintenance and updates of server software and hardware.
- Scheduled backups to ensure data integrity.
- Ongoing training for IT staff on crash recovery techniques.
- Implementation of monitoring systems to detect potential issues before they lead to crashes.

Related Policies and Documents

- *Student Handbook*
- *Data Protection Policy*

Communication

- *Orientations with students and parents*
- *School Website*
- *Student Handbook*

Policy Review Cycle

- This policy will be reviewed annually by the IT department and school leadership to ensure its effectiveness and updated based on technological advances and system changes.
- This policy was last reviewed by the RDOC in October 2024.