Business Continuity Plan (BCP)

**Organisation:** Holmview Primary  
 **Version:** 1.0  
 **Effective:** n/a  
 **Owner:** Principal  
 **Review cycle:** Annual, and after any major change or incident

# Table of Contents

[Table of Contents 1](#_Toc471349243)

[Purpose 1](#_Toc2136393564)

[Scope 2](#_Toc35395021)

[Assumptions 2](#_Toc628912337)

[Roles and Responsibilities 2](#_Toc490237501)

[BCP Activation 2](#_Toc1022078869)

[Triggers 3](#_Toc1615097052)

[Levels 3](#_Toc1987035936)

[Continuity Scenarios 3](#_Toc819768596)

[Cyberattack 3](#_Toc409398728)

[Loss of Site/Loss of Power/Internet Outage 4](#_Toc212713303)

# Purpose

To ensure that regular school operations can continue and be resumed as fast as possible during large disruptions. Such as cyber attacks, loss of power or external internet connection or a natural disaster. This plan is designed to be used with the disaster recovery & backup recovery policy document.

# Scope

* **People:** Students, staff, visitors, contractors, parents and volunteers.
* **Services:** Directory services and ldap, file sharing, printing, device management, email and CCTV servers.
* **Assets:** Any device or physical property that belongs to the school such as servers, buildings, networking devices, etc.

# Assumptions

* Google Workspace is available from offsite and will continue to function normally.
* That controls for risks are in place as per the risk register.
* Legal responsibilities such as child safety apply at all times.

# Roles and Responsibilities

* **Principal:** Approves the activation of the Business Continuity Plan, approves and decides on priorities and approves external communications.
* **Continuity Manager/Incident Commander:** Principal or a delegate of the principal, ensures that the business continuity plan is carried out effectively in a timely manner.
* **Business Manager:** Coordinates non-ICT continuity, writes and sends out communications to staff, parents and other key stakeholders.
* **ICT Director:** Carries out back restoration and other technical recovery as per the Disaster Recovery and Backup Policy.

# BCP Activation

This section details and describes situations which necessitate the activation of this plan. The principal can activate this plan for another reason not listed below for any reason. There are also different levels in which this plan can be activated, if it is not necessary to put the entire plan into action it should only be partially activated.

## Triggers

* **Cyber attack:** Ransomware, DDoS attack, large credential compromises, etc.
* **Loss of site:** When there is widespread damage to the site or it is unsafe to use the site for any reason such as: flooding, cyclone or a prolonged power outage.
* **Prolonged internet or cloud outage:** An outage that significantly affects student learning and the ability for staff to effectively do their job.
* **Destruction with malicious intent:** Any targeted or non-targeted attack that significantly damages computational, network or facility resources.

## Levels

* **Business as usual:** Regular business operations, risk levels are low
* **Standby:** In times where risk levels are higher than usual. Backups should be tested and verified as per the backup policy and BCP activation drills carried out.
* **Partial Activation:** Some services are down, BCP activated only for necessary areas. Backup recovery for some systems is done.
* **Full Activation:** When critical services are down for long periods of time or it is not safe to be onsite. Disaster recovery and backup procedures activated.

# Continuity Scenarios

## Cyberattack

* Affected systems and servers are isolated from unaffected ones in order to stop the spread of malicious code.
* If digital learning is not possible then student learning switches to paper based learning.
* Rolls are marked using a paper which will then be put into school management software at a later date.
* Critical payroll functions must be carried out via an alternative secure method.
* ICT systems restored from immutable backups
* Contact authorities such as OAIC if necessary
* Regular communications are sent to parents regarding the situation.

## Loss of Site/Loss of Power/Internet Outage

* Evacuation/closure of the school.
* Remote learning is put into place through google classrooms and google meet.
* Administrative staff operate from a designated alternative site or from home through the use of cloud-based management software.
* Temporary switch to other providers of services if necessary.