DISASTER RECOVERY AND BUSINESS CONTINUITY POLICY

Version	1.01	**Number of pages**	2
Responsible officer	Chief Operating Officer – Peter McCrindle		
Contact	Rob Corner – itmanager@morling.edu.au Ext: 110		
Approved by	Morling College Board		
Responsible body	Morling College Board		
Keywords	IT; ICT; Data security; Student records; Operations; Business disruptions; Disaster recovery; Systems		
Access level ***Select from the drop-down menu***	Public		
Dissemination Range	Staff and students		
Approval date	20 Feb 2023		
Effective date	20 Feb 2023		
Review date	20 Feb 2026		
Superseded documents	None		
Higher Education Standard	HES_6.2.1.i; 7.3.3.c		
Document classification ***Select from the drop-down menu***	Admin, Information Management, and Infrastructure		

1. PURPOSE

To ensure that Morling College maintains the security of data (including student records) and secure, reliable operations. This policy provides a framework for the management, implementation, and maintenance of plans, systems and services managed by Morling College in the event of disruptions to business continuity or security of data.

2. DEFINITIONS

Key Term or Acronym	**Definition**
Disaster Recovery and Business Continuity (DR)	A set of policies, tools and procedures to enable the recovery or continuation of vital technology systems following a disruption to the ICT. This includes the concept of Business Continuity through any disruptions which may occur
Information Technology (IT) or Information and Communications Technology (ICT)	IT and ICT are used synonymously in this policy and related documents to mean the systems and hardware which facilitate data management, communication and related information services

3. SCOPE

This policy applies to all individuals responsible for configuring, maintaining, and monitoring information systems of Morling College. Individuals may include Morling College employees, vendors, contractors, or managed service providers.

4. POLICY STATEMENT

Morling College will prepare and implement a comprehensive suite of plans to govern systems disaster recovery planning, preparedness, management, and mitigation of IT systems and services of any information.

5. PRINCIPLES

5.1 Whatever disruption affects the operation of MC, plans are enacted to ensure business continuity and quick recovery of access to systems, infrastructure and data required by the college and its stakeholders.

5.2 The Data Recovery and Business Continuity Plan will reviewed annually by the Chief Operations Officer and the National IT Manager.

6. RELATED DOCUMENTS AND LEGISLATION

Cyber Security Policy V2.00
ICT Disaster Recovery and Business Continuity Plan V3.00
Privacy Policy

7. REFERENCES

None

8. VERSION HISTORY

Version	Approved by	Approval Date	Effective Date	Changes made
1.01	Policy Coordinator	Feb 2023	Feb 2023	Keywords and HES reference added.
1.00	MC Board	20 Feb 2023	20 Feb 2023	New Policy

Download this policy anew with each use, as it may have changed.