Catholic Schools - BYOD Terms and Conditions

Section 1 - Purpose

(1) This document forms part of the Schools BYOD Guideline and sets out the terms and conditions under which the Catholic Diocese of Maitland-Newcastle (the Diocese) offers a "Bring Your Own Device(BYOD)" program at its schools. Its purpose is to describe the services and support offered to students using their own digital devices at school and the conditions under which those services and support are offered.

Section 2 - Scope

(2) These terms and conditions apply to all diocesan systemic schools within the Catholic Diocese of Maitland-Newcastle, all students at these schools and their parents and carers.

Section 3 - Responsibilities

ROLE	RESPONSIBILITIES
Students	• Adhere to the rules and policies defined by the Diocese and their school.
Parents/Carers	• Ensure their child has an appropriate device that is fit for purpose and properly set up according to the specifications and instructions provided. • Supervise and monitor their child's use of devices when not at school and assist their child to use devices effectively and responsibly.
The Diocese	• Enable effective learning through the use of personal digital devices at its schools by providing the necessary infrastructure, software and services. • Provide technical support to students using their own devices at school during normal school hours. • Assist students and parents/carers to understand and fulfil their responsibilities.

Section 4 - Terms & Conditions

Acceptance

(3) These terms and conditions are mandatory for anybody using a personal digital device at a diocesan school. Attempting to use a digital device at a diocesan school constitutes acceptance of these terms and conditions. If you do not accept the terms and conditions, contact your school immediately and not use or allow your child to use a personal digital device at school or for school work.

(4) Enrolling a device for Managed BYOD constitutes consent for the Diocese to manage the device. This allows the Diocese to provide an enhanced level of support, and also grants the Diocese authority to control the device as explained in the "Managed BYOD" section below. If you do not consent to the Diocese managing the device, do not enrol or allow your child to enrol the device for Managed BYOD.

Device specifications

(5) The BYOD minimum device specification is defined in a separate document, which is provided by the school. Some schools may require a specific model of device and may direct you to a specific supplier to purchase a device. Device owners are required to adhere to the specifications and processes applicable at their school.

(6) Devices must comply with the BYOD minimum device specification in order to be supported by the Diocese. Devices that do not meet the BYOD minimum device specification are not supported by the Diocese, cannot be enrolled for Managed BYOD, and might not work properly at the school. The Diocese may, at its discretion, provide some assistance but does not commit to any level of support for non-compliant devices.

(7) The BYOD minimum device specification is intended to ensure devices remain usable for several years, but as technology advances the specification may change from time to time. The Diocese may, at its discretion, continue to support devices that met an older version of the specification but are no longer compliant with the latest version. The Diocese decides what level of support it provides for non-compliant devices and when that support ceases.

Managed BYOD

(8) The term "Managed BYOD" refers to the use of a mobile device management service by the Diocese to control configuration and software on students' personal devices. This allows the Diocese to protect the security of its networks and student data, as well as ensure device settings and software are compatible and appropriate for use in its schools.

(9) Students can participate in Managed BYOD, in which case their devices will be managed by the Diocese. Managed devices will receive a higher level of support as described in the "Diocese Services and Support" section below. It is highly recommended that students participate in Managed BYOD.

(10) Parents/Guardians may elect not to participate in Managed BYOD, in which case their devices are "unmanaged" and receive a reduced level of support. This increases the risk of problems which the Diocese cannot resolve, and consequently the student might not be able to use the device effectively at school.

(11) To participate in Managed BYOD, students or parents/carers will "enrol" their devices as per instructions provided by the Diocese. Schools will ensure students and parents/carers have access to the instructions and assist them to understand and follow the process.

(12) Parents/Guardians may withdraw from Managed BYOD at any time by "unenrolling" their devices, in which case those devices become "unmanaged" and receive a reduced level of support.

(13) Enrolling a device for Managed BYOD grants the Diocese authority to do the following:

  a. Install and update approved software and digital certificates on the device.
  b. Change device configuration and settings.
  c. Remotely access the device in order to provide support or investigate a problem on request.
  d. Restrict access to sites and content deemed inappropriate.
  e. Monitor device usage and compliance with policies.
  f. Alter security settings on the device.
  g. Manage firewalls and intrusion detection systems.
  h. Apply encryption to protect the security of data stored on the device.
  i. Scan the device for viruses, malware, or any other potential threat to cyber-security.
  j. Remove any software, files, or data deemed to be a threat.
  k. Disconnect or disable the device in order to control a serious threat or cyber-security breach

l. Use location services to attempt to find a device reported as lost or stolen.

(14) Device owners can store their own data and install their own software on managed devices. The Diocese will not manage such data or software but will take action if a cyber-security threat is detected. This may include removing data or software and/or blocking the device from accessing school and Diocese networks and services.

Diocese Services and Support

(15) The Diocese provides services and support for managed and unmanaged devices as indicated below. All device owners have some responsibilities, but owners of unmanaged devices are responsible for more than owners of managed devices.

ACTION / SUPPORT	RESPONSIBILITY	
	Managed	Unmanaged
Acquisition of a suitable device and operating system	Device owner	Device owner
Loss or damage to devices and insurance cover		
Hardware or operating system malfunctions and/or warranty claims		
Home &/or mobile internet services and connectivity		
Personal Data storage and backup		
Any software not provided or supported by the Diocese/school		
Install, setup, and configure Diocese/school provided applications	The Diocese	
Software updates for Diocese/school provided applications		
Install and update anti-virus software		
Standard device configurations e.g. networks, updates, encryption		
Device security setup		
Device monitoring for compliance and threat detection		
Troubleshoot connection to School/Diocese networks		The Diocese
Limited troubleshooting of Diocese/school provided applications		

(16) The Diocese only provides technical support to students at school during normal school hours.

(17) The Diocese does not repair or replace any hardware or peripherals. This is the owner's responsibility and may be covered by a warranty or service provided by the manufacturer or supplier of the device.

(18) The Diocese will take due care but cannot be held responsible for any accidental data loss, corruption or damage that occurs in the course of providing services and support.

(19) Device technical data is collected and monitored by Diocesan systems, however, access to this data (and items like email, chat messages, etc) is restricted and only accessed when necessary – e.g. to protect a child's safety, or to provide technical support.

(20) The Diocese will not monitor web browser history or apply content filtering unless the device is connected to the Diocese's network infrastructure. The Diocese uses a reputable service to filter content accessed via its network but has no control over content accessed via other connections including home internet services.

(21) The Diocese provides high quality, reliable infrastructure and services, but cannot guarantee that access to its networks and services will always be available. The Diocese has processes and procedures in place to respond

effectively in the event of an outage and will take reasonable actions to restore services as soon as possible.

(22) On rare occasions, a problem may arise which can only be solved by performing a factory reset. This will remove all data, software applications, and settings from the device and return it to its original state. The Diocese will only perform a factory reset if absolutely necessary and will generally seek permission from the device owner before doing so.

(23) The Diocese provides services and support at its discretion and reserves the right to limit, modify or withdraw any and all services and support.

Parental Support and Supervision

(24) Parents/carers are expected to help and support their children as they learn and use their devices.

(25) Parents/carers are responsible for ensuring their children have a suitable device that meets the BYOD minimum device specification applicable at their school.

(26) Parents/carers are responsible for teaching their children to responsibly use and take care of their devices.

(27) Parents/carers are responsible for supervising and monitoring their children's use of devices whenever they are not at school. This includes ensuring recreational use is appropriate.

(28) Parents/carers are responsible for ensuring devices are properly set up in accordance with instructions provided by the school and/or Diocese. If assistance is required, parents/carers should contact the school.

(29) Parents/carers are responsible for helping their children resolve any problems with devices or software whenever they are not at school.

(30) Parents/carers are responsible for providing and supporting a home or mobile internet service that their children can use when not at school.

(31) Parents/carers are responsible for providing any required support, service, or action that is not provided by the Diocese or school.

Device Ownership, Usage and Care

(32) Devices always remain the property of the original owner whether managed or unmanaged.

(33) Devices must be registered using the student's school account, which is the account that the student must use to login when connecting to school networks and services.

(34) The Diocese is not responsible for any costs incurred by a device owner. There will be no reimbursement for any purchases, voice, data, or internet service charges, software licence fees, maintenance, repair, insurance, or other costs associated with the device.

(35) The Diocese is not responsible for any damage caused to a device by the owner or another student. The school may address behavioural elements such as careless or malicious acts, but the repair or replacement of a damaged device is solely the responsibility of the device owner.

(36) The device owner is responsible for obtaining insurance and warranties, and for making any claims. Some schools may offer advice or assistance, but the device owner is still responsible.

(37) The device owner is responsible for taking good care of the device and protecting it from damage while being used, stored, and transported.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Catholic Diocese of Maitland-Newcastle's Policy Portal for the latest version.

Page 4 of 7

(38) The device owner is responsible for maintaining the device and any installed software that is not managed by the Diocese.

(39) The device owner must use the device responsibly in accordance with the policies of the school and the Diocese, including the Information Security Management Policy and all related procedures.

(40) The device owner is responsible for making sure the device is fully charged each day before bringing it to school.

(41) The device owner is responsible for what is stored on and/or sent from the device and will be held accountable for any misuse including illegal or offensive material.

(42) Devices must not be used to take photographs or record audio or video of anyone without their permission.

(43) The device owner is responsible for removing any personal or sensitive information before disposing of the device, selling it, or giving it away.

(44) The device owner must not prevent or delay the installation of updates to the device operating system (e.g. Windows) nor to any software provided by the Diocese.

(45) The device owner must immediately inform the school if the device has been lost or stolen and take appropriate action to try to recover the device. E.g. If a device is left on the bus, call the bus company. If the device is managed by the Diocese, it may be possible for the Diocese to use location services to attempt to find a lost or stolen device.

(46) The device owner is responsible for labelling the device and device components for identification purposes.

(47) The device owner is solely responsible for backing up any personal data and personal applications stored on their device. CDMN is not liable for the loss of personal data resulting from device failure, factory reset, or any other technical issue.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Catholic Diocese of Maitland-Newcastle's Policy Portal for the latest version.
Page 5 of 7

Status and Details

Status	Current
Effective Date	27th October 2025
Review Date	27th October 2028
Approval Authority	Director Technology Services
Approval Date	22nd October 2025
Expiry Date	To Be Advised
Unit Head	Damian Wicks Director Technology Services
Enquiries Contact	Technology Services

Glossary Terms and Definitions

"Catholic Diocese of Maitland-Newcastle (the Diocese)" - The Catholic Diocese of Maitland-Newcastle (the Diocese) is inclusive of all parishes and agencies, communities, ministries and works that are under the authority of the Bishop of Maitland-Newcastle. The Bishop takes his authority from Canon Law (Canons 375-402). The geographical coverage of the Diocese includes all or part of the Newcastle, Lake Macquarie, Maitland, Cessnock, Port Stephens, Singleton, Muswellbrook, Upper Hunter, Dungog and Mid-Coast local government areas, with almost 160,000 Catholics, 38 parishes and serviced by multiple diocesan ministries and agencies. The Diocese is not wholly geographic in nature. There are elements of the Catholic Church operating within the physical boundaries of the Diocese that do not fall under the authority of the Bishop and are not a part of the Diocese. Equally, particular diocesan ministries occur within external institutions (e.g. Prison Chaplaincy, Hospital Chaplaincy).

"BYOD" - (Bring Your Own Device) – An arrangement allowing students at diocesan systemic schools to connect their own personal devices to school networks and use them for learning activities at school and at home.

"Content Filtering" - Restricting access to websites or content deemed to be harmful, offensive or inappropriate.

"Device" - A piece of electronic equipment that can receive, transmit, store and process digital information. Devices are typically laptop computers but can be any type of device used by a student including tablets, smartphones, smartwatches, and similar devices.

"Device owner" - The legal owner of a device or a student using a device provided by the legal owner.

"Hardware" - Physical components of a device.

"Managed BYOD" - An arrangement under which the Diocese uses a mobile device management service to monitor and control device settings and software. This enables the Diocese to provide a greater level of support and reduces the likelihood of problems using school networks and software.

"Managed Device" - A device that is enrolled for Managed BYOD and is consequently managed by the Diocese.

"Minimum device specification" - The minimum hardware, operating system, and general requirements for a device that can be used at a particular school.

"Operating system" - The software that is initially loaded onto a device and manages the device hardware and application programs. On most devices, the operating system is Windows.

"Peripherals" - Separate components that can be connected to a device, e.g. an external mouse or keyboard,

headset, stylus pen, etc.

"Unmanaged Device" - A device that is not enrolled for Managed BYOD and is consequently not managed by the Diocese.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Catholic Diocese of Maitland-Newcastle's Policy Portal for the latest version.

Page 7 of 7