BLACKFRIARS
PRIORY SCHOOL

DIGITAL TECHNOLOGIES POLICY

Date Approved: 2020

Review Date: August 2022

CONTENTS

CONTEXT

As the only school founded by the Dominican Friars in Australia, Blackfriars Priory School remains faithful to the search for Truth (Veritas) as lived and taught over the last 800 years by the Order of Preachers (Dominicans), and exemplified by Saint Dominic, our Founder, and Saint Albert the Great, our Patron.

Saint Dominic's commitment to study continued throughout his life. The pursuit of knowledge was not for its own sake but to better understand God's creation and its use in the works of the Order has continued through the centuries. Today, Dominicans can be found throughout the world.

An early member of the Dominicans was Saint Albert the Great. He became a lecturer, scientist, philosopher and Bishop. After his death he was recognised as a Doctor of the Church. The Doctor Universalis – The Universal Doctor, in recognition of his extraordinary genius and extensive knowledge, for he studied every branch of learning known at his time. His quest for knowledge saw him study everything he could find as it was through learning about creation, that he was able to know more about the creator, God, and then hand on that information to all he taught.

The lifelong commitment of Saint Dominic and Saint Albert to discovering and applying Truth to hand on to others remains at the core of the Blackfriars teaching pedagogy and its community. Blackfriars is built upon the Four Pillars of Dominican Life: Prayer, Study, Community Life and Service.

PURPOSE

The purpose of this policy is to articulate the position of Blackfriars Priory School in relation to Digital Technology practices at the School.

SCOPE

This policy applies to all members of the Blackfriars Priory School community.

POLICY

The School has established the Digital Technologies Policy to provide teachers, students and parents/caregivers with guidelines and instructions for the appropriate use of School-supplied and Bring Your Own Technology (BYOT) devices (including laptops, mobile phones, tablets etc.) and all Digital Technologies (including software and applications). All members of the School Community are expected to use Digital Technologies responsibly and ethically in all dealings with others.

The use of Digital Technologies supports student learning and enhances teacher delivery of the curriculum in the following ways:

- Digital devices are a valuable resource for facilitating access to information, the internet and online learning
- The creation and presentation of Student work is enhanced through the use of Digital Technologies (including all hardware and software)
- The responsible use of Digital Technologies is based on developing mutual trust and respect for other users
- Students need to be educated in the social skills and responsibilities associated with the use of Digital Technologies so as to enable them to assume their place in the adult world
- Students are personally responsible for their actions and interactions when using Digital Technologies (including the Internet and email)
- The use of Digital Technology resources at the School is a privilege, not a right.

STUDENTS

Students and their parents/caregivers must read and understand this policy before students are given permission to bring BYOT devices to school and/or make use of School-supplied technologies.

This policy also applies to students during excursions, camps and extra-curricular activities.

1. BYOT devices and uses (laptops and tablets)

1.1. Students may register a maximum of two devices (not including mobile phone devices) on the School network, each of which must be registered with a 'BYOT Device Registration Form' including the device's Wi-Fi MAC address.

1.2. The School offers a Preferred Device option though a school supplier and it is recommended that all students use a Windows-based machine as their main device, especially from Years 9 to 12. The advantages of a School Preferred Device include:

1.3. Onsite support at the School

1.4. Option of extended warranty and damage protection

1.5. Parents/caregivers should be aware of the Digital Technologies their son takes to school, including the device and also what software, applications and other files are stored on the device.

1.6. Minimum requirements for a BYOT device include:

1.6.1. **Battery** – Battery must last the duration of the school day, which is approximately 8 hours. Devices must be fully charged before they are brought to school. The use of power boards, extension cords and double adaptors are not permitted as they create a health and safety risk i.e. a trip incident. If the device does not last a full day, a second battery should be considered, if possible. Students are ONLY permitted to charge their device at school with the permission and supervision of a staff member AND if it is safety tag tested. Students may request that the School to safety tag test the device for them by making an appointment with a staff member in the Senior Library.

1.6.2. **Storage Capacity** – Most modern devices have adequate storage on their hard drive (minimum 120GB) or through additional SD storage cards or cloud storage. All students have access to OneDrive and the School expects that students use this for backing up and storage of school related files.

1.6.3. **Memory** – Devices should have a minimum of 4GB memory (RAM).

1.6.4. **Weight and size** – It is important that the device is able to be carried and stored easily to and from School and in-between classes.

1.6.5. **Wi-Fi** – Access to the School's network will be available through a Wi-Fi connection. It is important that students are able to access this on their device.

1.6.6. **Carry Bag and Label** – All devices must be carried in an appropriate case or bag that gives the device adequate safety. The bag, when carried around the School, must only be a satchel style bag for the laptop and charger and not a backpack. It should be plain and a dark colour such as black. It is also a requirement that each device be clearly labelled with the student's name. Devices must be stored in a locked locker when not in use.

1.6.7. **Accidental Damage Protection** – It is a requirement that all BYOT devices are covered by personal insurance or an optional accidental damage protection plan. It is advised that families contact their insurance provider if unsure. The School does not cover costs for loss or damage to these devices at school.

1.6.8. **Antivirus** – It is the responsibility of the student and their family to ensure that all devices have updated antivirus software installed.

1.6.9. **Passwords** – It is strongly advised that students use passwords/PIN to ensure that unauthorised activity cannot occur on their device (e.g. by other students or if stolen). Students must keep their passwords and PIN numbers confidential. Devices and/or passwords must not be shared.

2. Acceptance of Digital Technologies Policy & Procedures

2.1. All students and their parents/caregivers are required to read and sign the Acceptance of Digital Technologies Policy & Procedures Agreement prior to being able to access the School's network.

3. Theft, Loss or Damage

3.1. All devices must be clearly labelled with the student's name.

3.2. Students should leave their devices locked in their locker or bag when they arrive at school. To reduce the risk of theft during school hours, students who carry mobile phones are advised to keep them well concealed and not 'advertise' that they have them.

3.3. The School accepts no responsibility for replacing lost, stolen or damaged devices.

3.4. Devices that are found at the School and whose owner cannot be located will be handed to the Student Services Office.

3.5. Students are encouraged to activate mobile phone search applications such as "Find my iPhone" to support locating a lost or stolen mobile phone.

4. Mobile Phone Use

4.1. Mobile phones and/or other small personal devices must be switched off and kept in lockers (or school bags from Primary Students) from the 8:35am bell until students are dismissed at the end of the day.

4.2. Primary Students may give their mobile phone to their classroom teacher to lock in a secure location inside the classroom for the duration of the school day.

4.3. Secondary Students may provide their own lock to secure their locker. Students must provide access to staff to the locker when requested, or the lock will be removed at the discretion of staff.

4.4. The School does not take any responsibility for loss, damage or theft of personal electronic devices.

4.5. Parents/caregivers are reminded that in cases of emergency, the School's office is the vital and appropriate point of contact, and through this contact point the School can reach a student quickly and assist in any appropriate way.

4.6. Staff are expected to actively supervise and implement this policy.

4.7. Staff are expected to model appropriate behaviour with regard to mobile phone use. There will be instances where, especially during yard duty when exercising duty of care, staff will be required to use a mobile phone. Staff should not be on their mobile phone for personal use during lesson time or whilst on yard duty.

4.8. Students are not to wear headphones at any time whilst moving around the School, during lesson or break time. Students may be permitted to use headphones in class at the discretion of the teacher taking the lesson.

4.9. Where there is a specific learning purpose for the use of a mobile phone or small personal device required by the class teacher, the class teacher will explicitly request this of the students. The mobile phone will then be required to be immediately returned to the student's locker once the learning purpose task is complete.

4.10. Students should protect their phone numbers by only giving them to friends and keeping a note of who they have given them to. This can help protect the student's number from falling into the wrong hands and guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

4.11. Should a student breach this policy and have their mobile phone or other small personal device out of their locker or in view of staff during the school day, the following actions will take place:

4.11.1. **First breach**: The mobile phone will be taken directly to the Front Office by the student, under direction from the teacher. Upon arrival the mobile phone will be confiscated and secured in the Front Office in a zip lock bag with the student name written on the bag and logged through SEQTA. The mobile phone can be collected by the student at the end of the school day, after 3:15pm. A SEQTA direct message will be forwarded to the parent/caregiver warning of further consequences.

4.11.2. After the staff member sends the student to the Front Office, the staff member will, as soon as possible, complete a SEQTA alert specific to the mobile phone breach. This alert will be automatically sent to the Front Office. If the student fails to attend the Front Office, it will be reported to the Head of House for follow up with the student and may be treated as an additional issue.

4.11.3. Primary teachers will take the device and lock it securely in the classroom for collection at the end of the day.

4.11.4. **Second breach**: Same as for a First breach, and in addition the student will complete a Community Service and have a discussion with their Head of House or Home Group Teacher, at a time suitable for the staff member, in relation to their mobile phone use.

4.11.5. Primary teachers will take the device and lock it securely in the classroom for collection by parent/caregivers at the end of the day.

4.11.6. **Third breach**: Same as for a First breach, but the mobile phone will only be returned to a parent/caregiver and cannot be collected by the student. The student's Head of House will schedule a discussion with the student's parent/caregiver in relation to mobile phone use and any ongoing support the student may need. The student will complete a Long Community Service.

4.11.7. Primary teachers will take the device and lock it securely in the classroom for collection by parent/caregiver at the end of the day.

4.11.8. **Subsequent breach**(es) for the calendar year: Same as for a Third breach, except that the student will also be suspended from school for one day (in place of the Long Community Service) which will require a re-entry meeting with the parent/caregiver. A mobile phone management plan may be developed which involves the mobile phone being deposited in the Front Office at the beginning of each day.

5. Inappropriate Conduct

5.1. Any student/s caught using technology to cheat in exams or assessments will face disciplinary action as sanctioned by the Principal, Deputy Principal (Secondary) or other member of the School's leadership.

5.2. The supervising teacher may request all mobile phones be placed in a container at the front of the classroom on entry to the class. This will be the expectation in all exams. Students should only use their mobile phones before or after school or during recess and lunch breaks.

5.3. Any student who uses vulgar, derogatory or obscene language while using any digital technology will face disciplinary action as sanctioned by the Principal, Deputy Principal (Secondary) or other member of the School's Leadership Team.

5.4. Students must not engage in personal attacks, harassment of another person or post private information about any other person using SMS or other electronic messaging, taking/sending photos or objectionable images, and phone calls. Students using any means of technology to bully other students will face disciplinary action as sanctioned by the Principal, Deputy Principal (Secondary) or other member of the School's Leadership Team.

5.4.1. It is a criminal offence to use a device to menace, harass or offend another person. As such, the School may consider it appropriate to involve the police.

5.5. Students must not use Digital Technologies in a way that poses a risk to the School's network.

5.6. Students must not use Digital Technologies to photograph or film any student without their consent.

5.7. Digital Technologies are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to other students, staff or visitors to the School.

5.8. If there are repeated disruptions to lessons caused by a device, the responsible student may face disciplinary actions as sanctioned by the School's Leadership Team.

5.9. Content accessed through the School's network will be subject to monitoring and filtering and students must be aware that all use of internet and email is monitored and traceable to the student's account. This includes the use of mobile devices used on the School's network.

5.10. The School may block a student's access to the network if it is believed that they may be using the network or their device inappropriately. This includes (but is not limited to) accessing or storing inappropriate content, illegally installed software, bypassing school filters, use of VPNs,

misuse of email, forums, blogs, OneDrive or any other service provided by the School. A member of the School's Leadership Team can request the Systems Manager or a member of their team to audit a device.

5.11. All students' communication should be in appropriate formal written communication similar to writing a formal letter. Students are reminded that emails sent from the School using their School email address represent both themselves and the School.

SCHOOL STAFF

1. Ownership

1.1. The School may supply digital technology devices to its staff to use in the course of their employment.

1.2. The School is the owner of all:

1.2.1. ICT hardware that is supplied for use by staff and students; and

1.2.2. Digital content created and stored on the ICT facilities of the School by staff in the course of their employment. Provided such digital content is not confidential or commercially sensitive, the School will generally authorise Staff to retain a copy thereof for their own use.

1.3. The School at all times retains the right to:

1.3.1. Audit the digital content of all School-supplied ICT hardware (including content created, modified or received by staff both in the performance of their duties and through non-work related activities).

1.3.2. Monitor any Staff member's use of ICT facilities and ICT related activity both in the performance of their duties and through non-work related activities using School-supplied ICT hardware.

1.3.3. Take immediate possession of any School-supplied ICT hardware.

1.3.4. Make backups of digital content on School-supplied ICT hardware.

1.4. Whilst the School retains the rights listed above as it deems appropriate, the auditing and monitoring of ICT facilities will generally be limited to:

1.4.1. Ensuring ICT facilities, devices, systems and networks are functioning effectively.

1.4.2. Protecting against unauthorised use and access.

1.4.3. Ensuring compliance with this policy.

1.5. The audit and/or monitoring of ICT facilities and School-supplied devices must be authorised by the Principal.

1.6. Electronic communications are legally to be treated the same as printed or written communications.

1.7. Upon being assigned with a School-supplied device, Staff must read and sign a copy of this policy.

2. Device Responsibilities

2.1. All staff members are responsible for their School-supplied devices.

2.2. If a School-supplied device is lost or stolen, staff must inform a member of the Executive. The Executive may request that the staff member file a police report and/or provide a report number for insurance purposes.

2.3. All devices left overnight at the School must be stored in a secure place, preferably in a locked room away from student access.

2.4. Physical damage to School-supplied devices must be immediately reported to the ICT Department.

2.5. When a Staff member leaves their employment with the School, all School-supplied devices and accessories must be returned to the ICT Department no later than on the last day of employment. This includes School-supplied laptops, iPads, carry bags, charging cables and building fobs.

2.6. If Staff take leave for a period of longer than six months, any School-supplied devices may be temporarily reissued to the staff member's replacement teacher. The device must be returned to the ICT Department before being reissued.

2.7. Shorter periods of leave may require a temporary reissue depending on the availability of devices in the ICT Department.

2.8. If requested by the ICT Department's System Manager, Staff must, within the specified timeframe, return all assigned ICT hardware to the School's ICT Department for the purpose of replacement, repair or upgrade. Replacements, repairs and/or upgrades will generally be scheduled during school vacation periods in order to minimise the impact on student learning.

3. Content

3.1. At all times, staff are prohibited from using the School's ICT facilities and hardware to:

3.1.1. Discriminate

3.1.2. Abuse, vilify, defame, or harass

3.1.3. Purposely facilitate the viewing, receiving or sending of offensive, obscene or pornographic digital content

3.1.4. Seek to gain unauthorized access to any resource or entity, including another's accounts, logins, services, and/or system resources

3.1.5. Injure the reputation of or cause embarrassment to the School

3.1.6. Breach the intellectual property rights of the School or any other individual, group of individuals or organisation

3.1.7. Use software that has not been appropriately licensed

3.1.8. Use warez networks, torrents, peer to peer networking or to be involved in the sharing of files using these networks

3.1.9. Perform any unlawful act in compliance with State and Federal laws

3.1.10. Perform any inappropriate or offensive act including anything contrary to the Four Pillars of Dominican Life

3.1.11. Use VPNs or network activity anonymisers.

3.2. If a staff member unwittingly receives or views offensive, obscene or pornographic digital content, the content must be immediately deleted and a report must be made to the ICT Department's Systems Coordinator.

3.3. VPNs or network activity anonymisers may be installed by ICT leadership staff if it is used to assist with identifying server connections that other members of the School community are making, in particular students. It is not to be used in any other scenario.

3.4. At all times, staff must comply with all other School policies, procedures and Codes of Conduct when using the School's ICT facilities and hardware.

4. Personal Use

4.1. Staff members are permitted to use the School's ICT facilities and hardware for personal purposes, provided the personal use does not interfere with or negatively impact their work performance.

4.2. Staff members are not permitted to use the School's ICT facilities and hardware for commercial purposes that do not relate to the School.

4.3. Unless for educational purposes and linked to an education program or professional development, ICT facilities and hardware cannot be used during normal hours of work to access:

4.3.1. Game websites or video content related to gaming.

4.3.2. Gambling websites.

5. Email

5.1. All email correspondence is to be of a professional standard and should be written similar to the format of a formal letter.

5.2. Staff should not send emails to 'All Staff' email groups unless the matter is urgent, or if it is necessary for daily organisation purposes (including emails regarding important lost items).

5.3. Emails in relation to sports results are to be sent to the Co-Curricular Administrator (R-12) who will then inform the School community via the appropriate avenues.

5.4. Content related to professional learning and development is to be sent to the relevant Curriculum Leader or the Chair of the Professional Learning Committee, who will then inform Staff via the appropriate avenues.

5.5. The Principal is not to be carbon copied or blind carbon copied into emails regarding non-critical incidents unless the issue cannot be resolved at the relevant Executive level. However, any critical incidents must be reported to the Principal.

5.6. The use of the blind carbon copy email feature is prohibited, unless a list of recipients needs to be kept private for genuine reasons. For example, an email sent to multiple parents/caregivers should be sent via the BCC feature so that their email addresses are not shared amongst the recipients.

5.7. All emails sent and received are the property of the School and can be viewed by the Executive when reviewing professional conduct. This process must first be approved by the Principal.

6. Social Media

6.1. Staff must be aware of the risks associated with personal and professional use of social media, including but not limited to:

6.1.1. Information posted on social media is saved into the database of the platform being used, and may no longer be under the full control of the user.

6.1.2. Other users may screenshot and keep a permanent record of information posted on social media.

6.1.3. When content is deleted on some social media platforms, it may be kept in a database hidden from online viewing.

6.2. Staff using social media for professional learning and development must exercise professional conduct when posting information. This includes communicating in the same manner that staff would communicate with colleagues, Students and members of the School Community. Online behaviour in this setting can be representative of the School and, in particular, the culture of the School.

6.3. Staff must ensure their personal social media use does not compromise their role in the School community or the culture of the School. The following applies to personal social media use:

6.3.1. Staff social media accounts must be on the highest level privacy settings.

6.3.2. Staff are not to contact students through personal social media accounts. If contact is required, School email is an appropriate platform.

6.3.3. If a student contacts a staff member on social media about a genuine learning matter, the staff member may respond once only to correct the student about the process and refer the communication to the School email.

6.3.4. If a student contacts a staff member on social media about a matter that is unrelated to education, the staff member must not respond or engage. Staff must inform the Student's Head of House or, in extreme situations, the Assistant Deputy Principal, Wellbeing. This process is necessary to protect Staff from potential liabilities.

6.3.5. "Friend Requests" from current students using social media platforms must be rejected and the incident must be reported to the relevant Head of House.

6.3.6. Staff posts must be directed to a private audience. Public posts are acceptable if the social media account is not identifiable as belonging to a member of the School's staff.

6.3.7. Staff are personally responsible for the content they post. If a post or subsequent searches based on information in a post can identify staff as an employee of the School, staff must not post material that:

6.3.7.1. is confidential, offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, infringes copyright (or any other third party intellectual property rights), or is otherwise unlawful, or any other form of harassment or bullying as defined in the School's Code of Conduct; or

6.3.7.2. might otherwise cause damage to the reputation of the School, its staff, its students, the Dominicans or the Catholic Church, or bring any aspect of the School into disrepute.

6.3.8. Personal digital postings must not include the School's name or branding and must not include images of or references to specific students.

6.3.9. Staff must not post comments or upload images or information that would compromise the privacy or confidentiality of students in keeping with any obligations under the Privacy Act or potentially reflect adversely upon the School and its values.

6.3.10. Staff are not to make any negative or adverse posts or comments about the School or members of the School Community.

6.3.11. Staff are not to bully, harass or discriminate against or engage in other similar behaviour towards another Community member (cyberbullying).

6.3.12. Staff should not make posts or comments on social media platforms during times when they are expected to be working. Posts and comments are permitted during normal working break times.

6.3.13. It is recognised that staff may have friendships with parents/caregivers of students, which have formed outside of the School community. It is understood that social media "friendships" may exist. Professional communication must be conveyed when discussing School matters.

6.3.14. Conveying confidential School information via social media is strictly prohibited, regardless of the appropriateness of the receiver.

6.3.15. Staff are advised not to have old scholars as "friends" on social media platforms as this could result in a compromise of the reputation of the School community. If staff do "friend" old scholars on social media, the old scholar must be over the age of 18 and have been a graduate for over a year.

6.4. Teachers may communicate with students via social media if it is via a professional account on a platform solely used for education. Such communications may only be related to education and not personal events. For examples, teachers may use tools such as SEQTA and Edmodo to connect with students, but must not use Facebook or Twitter. The content must only be available to a private audience.

6.5. If a negative post or comment is found online about the School, a student or a staff member, and the post or comment is in a School-related context, online responses are strictly prohibited even if they are in defense of the scenario.

6.5.1. If the post or comment is made by a student, their Head of House is to be notified. Otherwise, an appropriate Executive member is to be immediately notified via email with a link to the relevant post or comment.

6.6. If a member of the media contacts staff about School related matters, they are to be referred to the Principal and no comments should be made. There may be situations where media coverage could promote the School; in this scenario the Principal is to be contacted for approval.

7. Privacy and Security

7.1. Staff will be provided with credentials to gain access to the School's digital technology facilities and digital content through user names and passwords.

7.1.1. Staff must not allow these credentials to become known or used by any other person.

7.2. Staff must not connect, or attempt to connect, to any digital technology facilities or digital content for which they have not been provided access. This includes:

7.2.1. Accessing the accounts of other Staff

7.2.2. Accessing or modifying digital content without authorisation

7.2.3. Transmission or disclosure of content without authorisation

7.3. Staff access to any digital technology or information should be only for that necessary for their role.

7.4. Transmission and disclosure of information to other staff is permitted if all parties involved are authorised to view the information or content.

7.5. Staff must take all responsible and appropriate steps to ensure the security of all digital content. Such steps include, but are not limited to:

7.5.1. Using passwords that are difficult for others to determine

7.5.2. Not sharing passwords with any other person

7.5.3. Logging into the School's digital technology facilities on trusted computers and networks only

7.5.4. Ensuring others cannot see the keyboard when typing in passwords

7.5.5. Locking or logging out of unattended computers

7.5.6. Physically locking digital storage devices away when not in use

7.5.7. Not using unauthorised software

7.6. Staff must not knowingly engage in activities that may cause damage to the School's digital technology facilities. In particular, the creation or transmission of viruses.

7.7. Logs of staff's digital technology usage will be retained by the School via the ICT Department. This content includes, but is not limited to:

7.7.1. Content of incoming and outgoing emails

7.7.2. Addresses, dates and times of Internet sites visited

7.8. Logs and backups are primarily used as a contingency plan to restore digital technology facilities. However, the Principal may authorise viewing to ensure compliance with this policy.

7.9. Staff must at all times adhere with the School's Privacy Policy and relevant privacy legislation.

7.10. The School will comply with relevant privacy legislation when enforcing this policy.

7.11. All Staff will read and comply with the Data Breach Response Plan within the Privacy Policy.

8. Copyright

8.1. Staff must not use or distribute any digital content that is subject to copyright or intellectual property law in any manner that is contrary to laws and regulations relating to copyright and intellectual property.

8.2. Any digital content that is copied to shared staff software and programs may be used by other Staff to deliver this content to classes.

8.3. Staff must seek approval before copying content that is not created by them from Staff Shares. Approval must come from the creator of the content or, if they are no longer employed or available, from the appropriate Curriculum Leader.

9. Investigation

9.1. In situations where a reasonable suspicion exists that a staff member has breached any provisions of this policy, the Principal can, in writing, authorise the:

9.1.1. Monitoring of a staff member's digital technology usage;

9.1.2. Audit of the digital content stored on ICT hardware by a staff member; and

9.1.3. Seizure of ICT hardware assigned to or accessed by a staff member.

9.2. For breaches that are considered minor, a less intrusive investigation process may be implemented.

9.3. If a staff member is to be investigated, they will be notified of the investigation.

9.4. When a staff member has been notified of an investigation, they shall be advised of the outcomes of such investigation upon its conclusion.

9.5. During any such investigation, the School shall adhere to the principles of procedural fairness and the Four Pillars of Dominican Life.

10.Disciplinary Action

10.1. When an investigation process concludes that a staff member has breached this policy, the staff member shall face disciplinary action, which may include, but not be limited to:

10.1.1. Access counselling;

10.1.2. Formal warning; or

10.1.3. Termination of employment.

10.2. In the event that the School believes that such breach of policy also constitutes a breach of the law, the School will notify the Police or other appropriate law enforcement agency. Contact may also be made with SA Police, SafeWork SA or the Teacher Registration Board, if necessary.

VISUAL TEXTS

1. Students aged under 15 years

1.1. Files that can be screened to students less than 15 years without consent are films rated G.

1.2. Teachers may also need to show PG rated films to secondary students for defined and programmed educational purposes. If a PG rated film contains material to which some parents/caregivers might conceivably object, it is appropriate to send a note to parents/caregivers with relevant information about the film and its classification and an invitation for them to contact the teacher if they have any concerns. Parents/caregivers' wishes must be taken into account.

1.3. Students aged less than 15 years should not view films with an M or MA rating. The MA category is a legally restricted category which prohibits students from viewing MA films unless in the company of a parent/caregiver.

2. Students aged 15 years and over

2.1. Students aged 15 years and over can view films rated G and PG without consent.

2.2. M and MA films should only be considered for students aged 15 years and over with consent of a parent/caregiver (excluding students aged 18 years and over). In this case it is adequate to send a note to parents/caregivers of students to whom it is planned to show the film, with relevant

information about the film and its classification and an invitation for parents/caregivers to contact the teacher if they have any concerns. Parents/caregiver' wishes must be taken into account.

2.3. It is not appropriate to organise student viewing of R rated movies even with parent/caregiver consent, regardless of the age of the student.

3. All Students

3.1. Discernment is required for all choices of movies.

3.2. Staff need to be aware of what beliefs are being promoted and how this engages with the Four Pillars of Dominican Life.

3.3. Students should be given the opportunity to compare and contrast the themes of the movie with the Four Pillars of Dominican Life.

DEFINITIONS

Audit	means to examine and assess the content of digital technology for compliance with this policy either by an authorised staff member or third party.
Backup	means a copy or duplicate version, especially of a file, database, program, or entire system, primarily retained for use in the event that the original is, in some way, rendered unusable.
BYOT	stands for Bring Your Own Technology, which includes digital technology devices that are owned by students and used at the School.
Digital Content	means all information contained within or accessed via ICT hardware including but not limited to software applications, documents, all forms of electronic communication, images, internet sites, web pages and database records.
Digital storage devices	are physical devices used for storing data. These devices generally connect via USB.
Digital Technology	is an electronic tool, system, device, or resources that generates, stores or processes data.
Hardware	refers to any form of digital technology that is a physical component. This includes, but is not limited to, desktop and laptop computers, printers, servers, network cabling and wireless network infrastructure, scanners, cameras, storage media.
ICT	stands for Information Communication Technology and is used interchangeably with the term digital technology.
ICT facilities	means all ICT hardware, software and digital content.
Normal hours of work	means the period of time between staff's scheduled commencement and finish times on any day of work but excluding meal breaks.
Post	is when a user puts information online using social media, and the user's name is usually attached to this information.
Preferred Device	refers to a device that is offered to students for purchase from a School supplier.

Social media	is the use of websites and applications that enable users to create, comment and share content or to participate in social networking, usually online. Social networking generally involves, but is not limited to, maintaining a personal or professional profile online, which is used for commenting or sharing content. Online gaming networks and picture sharing applications are also considered forms of social media.
Software	refers to the programs and operating system that run on a computer. Software consists of data and computer instructions, as opposed to hardware which refers to physical components.
Staff shares	are network locations provided by the School as digital storage devices. These are accessed via the network and are shared by all staff.

RELATED DOCUMENTS/LINKS

1. IOCANE Web Portal – https://onetoone.iocane.com.au/
   (please email byot@bps.sa.edu.au for login details if required)
2. Department for Education South Australia – www.education.sa.gov.au
3. Data Breach Response Plan – BPS SEQTA Data Breach Response Plan 2020
4. CESA ICT Policy Collection –
   https://online.cesa.catholic.edu.au/docushare/dsweb/View/Collection-4238
   - 4.1. CESA Cloud Computing Policy
   - 4.2. CESA ICT Acceptable Use Policy
   - 4.3. CESA ICT Acceptable Use Guideline
   - 4.4. CESA Information Security Policy
   - 4.5. CESA Information Security Framework
   - 4.6. CESA Information Security Classification Guideline

POLICY IMPLEMENTATION

Responsibility for implementation, monitoring and review of the policy is vested at the level of the following roles:

ICT Team

School Executive

POLICY REVIEW

Frequency:	Every 2 years
Next review date:	August 2022

APPROVAL AUTHORITY / POLICY OWNER

Blackfriars Priory School