## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vision and Rationale of the BYOD Programme</td>
<td>2</td>
</tr>
<tr>
<td>Ownership</td>
<td>3</td>
</tr>
<tr>
<td>Cost</td>
<td>3</td>
</tr>
<tr>
<td>Device Specifications</td>
<td>4</td>
</tr>
<tr>
<td>Procedures and Guidelines</td>
<td>4</td>
</tr>
<tr>
<td>Care of Devices</td>
<td>5</td>
</tr>
<tr>
<td>Loss and Damage</td>
<td>6</td>
</tr>
<tr>
<td>Faulty Devices and Technical Support</td>
<td>6</td>
</tr>
<tr>
<td>Use and Security</td>
<td>7</td>
</tr>
<tr>
<td>Virus Protection</td>
<td>7</td>
</tr>
<tr>
<td>Internet Usage</td>
<td>7</td>
</tr>
<tr>
<td>Social Networking</td>
<td>8</td>
</tr>
<tr>
<td>Inappropriate Use</td>
<td>8</td>
</tr>
<tr>
<td>Cyber Bullying</td>
<td>9</td>
</tr>
<tr>
<td>Internet Crime</td>
<td>9</td>
</tr>
<tr>
<td>Networks and Network Security</td>
<td>10</td>
</tr>
<tr>
<td>Software, Copyright and Intellectual Property</td>
<td>10</td>
</tr>
<tr>
<td>Non Educational Applications or Files</td>
<td>11</td>
</tr>
<tr>
<td>Security and Storage</td>
<td>11</td>
</tr>
<tr>
<td>Power Issues / Battery Use</td>
<td>11</td>
</tr>
<tr>
<td>Backup and Data Storage</td>
<td>12</td>
</tr>
<tr>
<td>Printing</td>
<td>12</td>
</tr>
<tr>
<td>AC Adaptor</td>
<td>12</td>
</tr>
<tr>
<td>FAQ 1: How much reliance is there on technology in the classroom</td>
<td>13</td>
</tr>
<tr>
<td>and can my child still learn without a device?</td>
<td></td>
</tr>
<tr>
<td>FAQ 2: How secure will my child's device be at the College?</td>
<td>13</td>
</tr>
<tr>
<td>FAQ 3: What will happen if my child breaks the device?</td>
<td>14</td>
</tr>
<tr>
<td>FAQ 4: What if we cannot afford the initial cost of purchase?</td>
<td>14</td>
</tr>
<tr>
<td>FAQ 5: What happens if my child's device becomes infected with a Virus/</td>
<td>14</td>
</tr>
<tr>
<td>Malware?</td>
<td></td>
</tr>
<tr>
<td>FAQ 6: Will my child be able to print at the College with their own</td>
<td>14</td>
</tr>
<tr>
<td>device?</td>
<td></td>
</tr>
<tr>
<td>FAQ 7: Will my child's personal data on the device be secure?</td>
<td>15</td>
</tr>
<tr>
<td>FAQ 8: How will my child be safe online at school?</td>
<td>15</td>
</tr>
<tr>
<td>FAQ 9: How will inappropriate internet usage be controlled at school?</td>
<td>15</td>
</tr>
</tbody>
</table>
2 VISION AND RATIONALE OF THE BYOD PROGRAMME

In 2008 the Commonwealth Government instituted its Digital Education Revolution (DER), designed to bring about a 1:1 computer to student ratio for Years 9 to 12 in Colleges by 2012.

With the demise of funding of the DER program by the Australian Government, we have examined ways of extending this ratio to our Year 7 and 8 students.

The solution we have decided on is the “bring your own device” or BYOD solution.

Bring your own device (BYOD) refers to a technology model where students bring a personally owned device to College for the purpose of learning. These devices will enable students to access the internet and/or College network by Wi-Fi.

Many educators point out that personal devices are a very significant part of students’ lives. They argue that as these devices are integral to the world in which these students live, they should be integral to their learning lives and their use will make learning part of their lives.

BYOD allows students access to the same devices at College and at home and it can extend learning opportunities to times and places outside of the classroom.

BYOD will also allow students to work with technology with which they are already comfortable and familiar.

21st Century skills are cited by many educators as a justification for BYOD. They argue that we have come to a time when we need to accept the fact that the concept of 21st century skills is no longer a progressive phase to latch onto but a reality that we need to instil into our College systems.

These educators see that mobile devices are part of 21st Century living and integral to learning 21st Century skills. Learning becomes easier to achieve, as it is more collaborative.

More personalised, student centred learning is often cited as a reason for BYOD. Bring your own device puts students in a position of power over their learning. Many educators argue that giving students the authority over their own learning is best: the teacher becomes a manager of learning, rather than a direct source of information.

Such devices, in the hands of students, affords learning opportunities that bridge the formal learning with the informal, outside of classrooms. Many educators also argue that this and the ability to use their own device, leads to increased motivation and engagement.

“The cloud” enables any student with a device able to browse the web to store and share information and access applications. With browser-based apps, we don’t need to find and update resources and applications that are compatible with a wide range of devices and operating systems.

Other educators comment that parents are realising that a digital device is necessary for learning.

Within the Melbourne Declaration on the Educational Goals for Young Australians (MCEETYA 2008) it is recognised that in a digital age, and with rapid and continuing changes in the ways
that people share, use, develop and communicate with Information Communication Technology (ICT), young people need to be highly skilled in its use.

To participate in a knowledge-based economy and to be empowered within a technologically sophisticated society, students need the knowledge, skills and confidence to make ICT work for them at school, at home, at work and in their communities.

Students develop ICT capability as they learn to use ICT effectively and appropriately to access, create and communicate information and ideas, solve problems and work collaboratively in all learning areas at school, and in their lives beyond secondary education.

This capability involves students in learning to make the most of the digital technologies available to them, adapting to new ways of doing things as technologies evolve and limiting the risks to themselves and others in a digital environment.

3 Ownership

The 1 to 1 initiative is a ‘parent purchase’ model. In this model, the device will be owned by the family and students. Parents / caregivers of students are encouraged to insure the device and this is a responsibility that will remain with the parents.

4 Cost

The cost of the device is $650 (inc.GST). There will be three options for parents to consider:

- **Upfront purchase**
  - Cost $650

- **Monthly Payments of $58 per month over 12 months**
  - Cost $696

- **Rent the Device at $260 per year over 3 years**
  - Cost $780

Please note with the rental option, the College retains ownership of the device and there is no option to purchase at the end of the rental term i.e. the device will need to be returned to the College at the end of the rental period.

Parents will need to sign the accompanying contract before the device is issued.
5 DEVICE SPECIFICATIONS

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model name</th>
<th>SW5-012-1774</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acer</td>
<td>Aspire Switch 10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU type</th>
<th>OS</th>
<th>RAM</th>
<th>WLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Atom Z3735F</td>
<td>Windows 8.1</td>
<td>2048 MB</td>
<td>802.11a/b/g/n + BT</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Display Size</th>
<th>Flash Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1&quot; FHD Multi-Touch LCD</td>
<td>64 GB</td>
</tr>
</tbody>
</table>

6 PROCEDURES AND GUIDELINES

Prior to devices being issued to students:

Parents will need to sign a Device Agreement Form agreeing to the terms and conditions of the program.

Parents will need to complete a Payment Options Form advising which of the three purchase/rental options they have chosen. Please note that if payments are to be made by Direct Debit, Credit Card or Centrepay a separate authority will also need to be completed. In the case of the rental option being chosen, a Rental Agreement will also be required.

Each device will be registered in the school database with a unique barcode identifier against the student's ID. This will be important for security, repairs and warranty purposes.

Students will participate in further induction to ensure that they are familiar with their roles/responsibilities by Pastoral Care and subject teachers.

The device must be brought to school fully charged and ready for use in classes each day. There will be no charging facility for student devices at school. Students who fail to bring their fully charged device to school will need to use traditional writing materials on that day. When not in use the device must be stored in the student locker with the school supplied lock closed (Bosco Campus) and in the classroom (Benedict Campus). This includes all break times, PE, Art, Music, Design and Technology practical lessons and sports training. The device must be taken home each evening and must not be left in the locker or classroom overnight.
7 CARE OF DEVICES

Devices should be switched off at the end of every lesson before moving to your next class.

It is highly recommended that you use the protective carry case that comes with the device.

Try to avoid moving your device around when it is on. Before switching it on, gently place your device on a stable surface and then switch it on.

You still need to be careful with the device while it is in your bag. Do not drop your bag from your shoulder. Always place your bag gently down.

Be careful when putting the device in the car or bus that no other items are on top of it and nothing will roll on to the device bag.

Devices should be switched off before being placed into your bag.

Operating conditions

Please do not place objects on top of your device and never carry it around while it is turned on. Avoid exposing your device to:

• Direct sunlight or sources of heat such as desk lamps
• Dust, dirt, rain, liquids or moisture
• Heavy shock or vibration

LCD Screens

LCD screens are delicate - they don't like being poked, prodded, pushed or slammed. Never pick up your device by its screen. Don't slam the screen closed and always be gentle when putting your device down. Ensure that nothing is left on the keyboard before closing the lid. Serious, expensive damage to the screen may result if the check is not done.

To clean your LCD screen:

• Switch off your device
• Lightly dampen a non-abrasive cloth with water and gently wipe the screen circular motion.
• Do not directly apply water or cleaner to the screen
• Avoid applying pressure to the screen
8 **LOSS AND DAMAGE**

Parents/Caregivers need to ensure that the device is covered under their home/contents insurance policy at all times.

It is the user's responsibility to report lost or stolen devices to the nearest police station and provide the insurer with a crime report number and claim for a replacement on their Home Contents or Car Insurance. If the device is taken overseas, please ensure that it is covered by travel insurance.

If a device is damaged in any way it should be reported immediately to your Caregroup teacher at Bosco Campus or your class teacher at Benedict Campus or one of the ICT Staff.

The cost of all non-warranty repairs to damaged devices will be the responsibility of the parents/caregivers.

9 **FAULTY DEVICES AND TECHNICAL SUPPORT**

Technical support is available through the ICT Centre. A loan device *may* be provided in cases where the device cannot be repaired on that day.

If the computer has an obvious hardware fault (screen or keyboard not working) then it should be reported directly to the hardware vendor (Acer). All warranty and hardware repairs must be done by Acer technicians, on-site, at St Mark's.

Acer Contact Details

*Acer Care Protection Plan Enquiries:* 1300 365 100  
7:00am to 9:00pm Monday to Friday AEST  
9:00am to 6:00pm Saturday and Sunday AEST  

*Technical Support:* 1300 365 100  
7:00am to 9:00pm Monday to Friday AEST  
9:00am to 6:00pm Saturday and Sunday AEST

*Service and Repair Enquiries:* 1300 365 100  
7:00am to 9:00pm Monday to Friday AEST  
9:00am to 6:00pm Saturday and Sunday AEST
10 Use and Security

The device must be brought to school fully charged and ready for use in classes each day. Students who fail to bring their fully charged device to school will need to use traditional writing materials on that day. When not in use the device must be stored in the student locker with the College supplied lock closed.

This includes all break times, practical lessons and sports training. The device must be taken home each evening and must not be left in the locker or classroom overnight.

11 Virus Protection

Anti-Virus software is built into Windows 8.1 Updates of this software will be automatic.

The devices also come with a trial version of MacAfee anti-virus software. It will be up to the user to extend this trial.

Students need to take all steps to protect the device from virus attacks.

Viruses can enter devices through:

- Removable media
- Emails
- The Internet (including web browsing, FTP programs and chat rooms)

**Tips**

- Do not open any files attached to suspicious or unknown emails
- Exercise caution when downloading files from the Internet. Save the files to the device's hard disk and run the virus scanner on the files before opening them
- Delete chain and junk emails. Do not forward or reply to any of these
- Never reply to Spam
- Hundreds of viruses are discovered each month. Run your virus scan regularly.

12 Internet Usage

Students can access the Internet through the College’s wireless network while on site. Access to the Internet through the College's network at College is monitored and subject to strict filtering. Students are not permitted to access the internet through any external device while at the College.

Students may also use the Internet for their personal use at home after setting up the device to access it through their home Internet Service Provider. (Consult your ISP for processes to do this).
There are significant educational benefits of some Social Networking applications. These sites allow users to interact with other users. These include web-based communities, hosted services, web applications, social-networking sites (Facebook, Twitter etc), video-sharing sites, wikis and blogs.

However, many Social Networking applications can be unproductive and distracting to student learning.

Educational technologies will be used as part of a student's study in various classes. The use of Social Networking applications are based on the policy that:

- The technologies, and the use of the technologies, do not breach any ethical and moral issues
- The applications do not distract student learning
- The Social Networking technologies are not to be accessed at school, unless specifically directed by the teacher for educational purposes
- Facebook is blocked by default when students access the Internet at school

The following guidelines are outlined to ensure all users are able to access the latest research available with the latest technology in an acceptable and safe learning environment.

- Users will avoid site with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way.
- Engaging in chat lines or downloading files is not permitted unless forming part of legitimate class activity guided by the teacher of that class.
- The Federal Communications Act determines guidelines for appropriate use.
- Inappropriate use of the internet and email is a serious matter and can have significant consequences, eg sending a message over the internet using someone else's name.
- Passwords should remain confidential. No user should log-on as another student using their password.
- Do not use inappropriate or offensive names for files or folders.
- Do not bring to College, or use, games or any other materials which may be offensive to others.
- Do not engage in cyber-bullying or a-crime.
- No device (or mobile phones) with camera capabilities are to be used in the classroom unless instructed by or with the permission of staff.
- Under privacy legislation it is an offence to take photographs of individuals without their expressed permission and place these images on the Internet or in the public forum.
15 Cyber Bullying

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways.

Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies such as email, chat room discussion groups, instant messaging, WebPages or SMS (text messaging) - with the intention of harming another person.

Examples can include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Activities can include flaming (repeated negative messages), trolling, sexual or racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking. The targeted person is required to inform the appropriate College authority.

Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life.

16 Internet Crime

Cyber bullying can therefore be an e-crime, a fact often not clearly understood by those involved.

E-crime occurs when a computer or other electronic communication devices (eg mobile telephones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

Consequences

Any form of cyber bullying or e-crime will be dealt with through the College's 'Harassment Policy'. Serious breaches are a police matter and will be dealt with through State and Federal laws and SA Police.
17 NETWORKS AND NETWORK SECURITY

Ad-hoc Networks:
Ad-hoc networks (the creation of a standalone wireless network between two or more devices) are strictly forbidden while at school.

Hacking:
Hacking is a criminal offence under the Cyber Crime Act (2001). Any hacking attempts will be forwarded to the police.

Packet Sniffing:
Any type of software or hardware device designed to capture or view network data/packets is forbidden.

18 SOFTWARE, COPYRIGHT AND INTELLECTUAL PROPERTY

Each device will have an image pre-installed.

The image will contain the Windows 8.1 operating system as well as other trial software.

Through this system students will be able to download the latest version of Microsoft 365.

Students may also be asked to download applications from the Microsoft Store as directed by staff. The majority of these apps will be free.

Students may add their own private software as required or directed by the teaching staff. This software must be legally purchased with a user license. Student added software must not be malicious or offensive or breach copyright laws.
19 Non Educational Applications or Files

The College does not object to the installation and storage of non-educational content and files on the device provided that the installed content:

- Is appropriately licensed (i.e. does not breach copyright and intellectual property laws this includes video and music downloads)
- Is ethically and morally acceptable (including consideration of school appropriateness, age appropriate ratings and privacy issues)
- Does not affect the efficient functioning of the devices for educational purposes (i.e. they do not interfere with the speed and storage capacity of the device or the problems that might arise from increased battery use)
- Does not affect the school's wireless network
- Does not interfere with the classroom learning program

Please note:

- The use of network games at school is banned
- No ad-hoc networks are to be formed

20 Security and Storage

The device is primarily for classroom and homework use. It should not to be used during recess and lunch. During practical classes, the devices should be securely stored in their locker or classroom.

21 Power Issues/Battery Use

Students must come to school with their devices fully charged.

New technology gives much longer life to modern batteries in computers. The Acer Switch10 has a battery life sufficient to last the school day.

It is recommended that you use the device on the inbuilt power-save setting for optimum battery life.
22 BACKUP AND DATA STORAGE

It is important to keep backups of critical student work. There are a number of options students should consider.

Work should be stored to the student’s One Drive.

Work should also be regularly backed up to a USB device, a portable USB hard drive.

The College will not be held responsible for lost work due to a failure to do backups.

23 PRINTING

Student work will mostly be electronically submitted. If you are requested to hand up a printed version printing facilities will be available at the school.

At home you may need to save your work to a USB storage device and print from a computer connected to a printer. You may also want to install your home printer to the device.

24 AC ADAPTOR

Connect your adaptor only to your device.

Do not step on your power cord or place heavy objects on top of it. Keep your cord away from heavy traffic areas.

When unplugging the power cord, pull on the plug itself, rather than the cord. Do not wrap your cord too tightly around the adapter box.

Be aware of the power savings that come from running your device effectively from battery after being fully charged. This can amount to a significant amount per year.

If you lose or damage your AC Adaptor please order a new one.

Do not use any other charging device as it may seriously damage your device.
25 FAQ 1: HOW MUCH RELIANCE IS THERE ON TECHNOLOGY IN THE CLASSROOM AND CAN MY CHILD STILL LEARN WITHOUT A DEVICE?

Students are able to learn without a device but learning how to work anywhere/anytime, have access to their resources 24/7, collaborate with others from anywhere and at any time, is only possible if students are connected and have a device. Devices can be used in 4 ways.

1. Substitution - Same task. New technology replaces old technology.
2. Augmentation - Same task. New technology increases functionality.
3. Modification - Staff are able to re-design part of the task.
4. Redefinition - Staff create new tasks once unimaginable.

If the only function of technology was substitution, then students can certainly survive fully engaged without a device. However, as teachers use technology to augment, modify and redefine tasks, a device becomes the ticket to full participation. If the school goes this way, we will have to provide access to devices for those who are genuinely unable to BYOD.

26 FAQ 2: HOW SECURE WILL MY CHILD'S DEVICE BE AT THE COLLEGE?

We will also record the serial number and model of each student device in a database for easy identification.

Students are encouraged to store their device in their lockers at recess and lunch at Bosco Campus and in their classroom at Benedict Campus.

Devices should also be stored in these places when the learning does not require the presence of these devices (such as practical lessons – PE etc.)

Students must take home the device each night. Under no circumstances should the device be left on school grounds after 3:30 pm.
27 FAQ 3: **WHAT WILL HAPPEN IF MY CHILD BREAKS THE DEVICE?**

The College strongly recommends that parents contact their household contents insurance provider to determine appropriate insurance coverage. It is also recommended, that should you purchase a new device for your child that you should enquire about accidental damage protection (ADP).

If the device is sent for repair, the College may provide the student with a spare device and charger if one is available.

If the device is still covered by an active manufactures or extended warranty, the owner of the device can lodge a warranty claim as per the original warranty agreement with the supplier.

28 FAQ 4: **WHAT IF WE CANNOT AFFORD THE INITIAL COST OF PURCHASE?**

Parents can rent the device from the College. For further details please contact the Business Manager, Dominic LoBasso.

The College recommends that the student's keep their anti-virus/anti-malware software up to date and run regular scans. The devices come pre-installed with a month’s trial McAfee Anti-Virus.

29 FAQ 5: **WHAT HAPPENS IF MY CHILD'S DEVICE BECOMES INFECTED WITH A VIRUS/MALWARE?**

Students can upgrade their subscriptions to McAfee or source their own anti-virus software.

The ICT Staff can be approached for guidance with this matter.

30 FAQ 6: **WILL MY CHILD BE ABLE TO PRINT AT THE COLLEGE WITH THEIR OWN DEVICE?**

The College will have printing facilities for students.
31 FAQ 7: Will my child's personal data on the device be secure?

Student data is only as secure as the strength of their password. It is recommended that students have a strong password for their device as well as any cloud service that they store any information on. Teaching students to manage a password is an important life skill. Staff will emphasise with all users that the moment they feel their credentials have been compromised, they must change their password.

Hand in hand with this, we hold our students responsible for any activity conducted via their account.

32 FAQ 8: How will my child be safe online at school?

The College internet access is filtered because of the nature of the internet, that doesn't guarantee that your child cannot gain access to inappropriate material. Even the fact that your child has an email address means that it is possible for them to be sent mail or shared into a document by someone with less than noble intentions.

We feel that educating students in Cyber-safety is essential, and will enhance each individual's awareness of potential malicious content or users.

Parents are also encouraged to discuss these issues with their children.

33 FAQ 9: How will inappropriate internet usage be controlled at school?

The College provides a strict internet filter and has an Acceptable Use Policy (AUP). Acting lawfully, safely and with consideration for the community is at the heart of our AUP.

For more information please get in touch with the ICT Staff at the college.