APPENDIX 2

John Wollaston
ANGLICAN COMMUNITY SCHOOL

BRING YOUR OWN DEVICE (BYOD) PROGRAM 2021
INFORMATION FOR YEARS 10 to 12

BRIGHT FUTURES

TABLE OF CONTENTS

1. INTRODUCTION

Vision

The John Wollaston Anglican Community School (the School) will make meaningful use of information and communications technology (ICT) to empower learners and to enrich and enhance learning experiences for all.

The School's BYOD Program is a wonderful opportunity for our students in Years 10 to 12 to access and utilize the latest technology, empowering them to become literate, self-directed learners and productive members of a technology-oriented society.

2. RESPONSIBILITIES

2.1 THE ROLE OF STUDENTS

Students must use their Device in accordance with the overarching *ICT Appropriate Use Policy: Students*. A copy of this policy is to be signed and returned by the student and Parent/Guardian.

It is recommended that no additional software, games or applications be installed on the computer as this can affect performance. Any additional software that is installed must not be left open or visible whilst at School. This includes desktop icons or shortcuts showing on the taskbar. Students who do not adhere to this condition will be in violation of the *ICT Appropriate Use Policy: Students*.

2.2 THE ROLE OF PARENTS AND GUARDIANS

Parents/Guardians are expected to understand and discuss with their child the content of this information booklet and accompanying documents. Parents/Guardians are expected to monitor their child's home usage of the Device, to ensure information accessed is in accordance with the *ICT Appropriate Use Policy: Students*.

2.3 THE ROLE OF STAFF

School teaching staff will provide training and opportunities within the curriculum for students to use the Device as an educational tool. Staff will monitor how the students use the Device to ensure material accessed complies with the *ICT Appropriate Use Policy: Students*.

2.4 THE ROLE OF THE SCHOOL

The School commits to upholding the *ICT Appropriate Use Policy: Students* and providing appropriate physical and financial resources to enable safe, educationally relevant access to the Devices and suitable curriculum facilities for staff and students.

3. STUDENT DEVICE

3.1 THE DEVICE

Students will require a MacBook or Windows device that complies with the specifications developed by the Manager of ICT Services. Please note that these are subject to change. Current specifications are available on the SEQTA ICT Portal.

3.2 SOFTWARE

The term 'software' describes the programs that are available for use on the Device.

The software required by students is available from links on the SEQTA ICT Portal. It is necessary to download and install the required software before using the Device in the classroom. It is not expected that further software will be required; however, should this be necessary in the second or subsequent years, Parents/Guardians will be notified in advance of any additional software or upgrade. No additional costs will be incurred if this is required.

Students are expected to maintain the software and operating system through regular updates that are made available by the manufacturer.

3.3 SOFTWARE LICENSING

The School has a legal and moral obligation to ensure the proper purchase and correct use of software occurs within its community. In order to achieve these outcomes, it must rely on community members' adherence to the appropriate School policies.

Software licenses have specific conditions of purchase. To satisfy the School's software licensing conditions of purchase, it is imperative that:

- School-owned software is **not** loaded onto home computers unless specifically allowed;
- In the event that the student leaves the School, any software licensed to the School on the Device is immediately uninstalled.

Note: In signing the *ICT Appropriate Use Policy: Students,* parents/guardians acknowledge and agree to the Licensing Conditions under which the software is provided.

3.4 PRINTERS AND OTHER PERIPHERALS

Printers will be made available to BYOD Devices through the use of a printing portal website. Details of this website can be found on the SEQTA ICT Portal page.

Families may wish to install their own printer/scanner drivers so that students can print at home.

4. TECHNICAL SUPPORT

4.1 TECHNICAL SUPPORT – IT HELP DESK

The School IT Help Desk (located adjacent to the entrance of Upper Primary Building) is open on weekdays (including School holidays) from 8:00am to 4:00pm, allowing students to seek technical assistance regarding their Device computers when necessary.

The IT Help Desk staff will attempt to help with all software issues on all BYOD Devices, however, will advise the student/Parent/Guardian of faults that lie outside the scope of the School to repair (for example hardware damage or failure).

If a temporary replacement device is required, this can be arranged through the IT Help Desk. The IT Help Desk can be reached on: support@jwacs.wa.edu.au or 08 9495 8130.

4.2 IT HELP DESK SERVICES

The School's IT Help Desk technicians endeavour to provide the following support:

- Answer queries pertaining to Information Technology at the School;
- Assist students with device technical issues.

4.3 SOFTWARE ISSUES

Students experiencing difficulties in using a software application on their Device, during class time, may be instructed by their teacher to take their Device to the IT Help Desk. Written permission from their classroom teacher is required.

4.4 DATA MANAGEMENT

The School will provide a OneDrive account for students to save their work. Saving and backup of personal data is the students' responsibility. Methods of data storage and backup will be demonstrated to students.

The School will not be responsible for the loss of data if a device needs to be repaired.

4.5 HOME INTERNET AND NETWORK CONNECTIONS

If a device is to be configured to run on a home network, it is possible that conflicts with the School's network configurations may occur. The IT Help Desk may be able to provide further information to aid in this configuration process.

5. LOAN DEVICES

The School may provide a replacement device whilst the student's assigned machine is being replaced or repaired. The School provides loan computers (subject to availability) for day use. Loan Devices may be available for overnight use with the class teacher's approval.

6. VIRUS PROTECTION

Students are expected to have suitable antivirus protection (for example Windows Defender) running and being updated. If students suspect their Device has become infected, they are to inform the IT Help Desk promptly.

7. MONITORING OF USE BY THE SCHOOL

As per the *ICT Appropriate Use Policy: Students*, the School reserves the right at any time to check work, email or data on the School's computer network, Internet access facilities, computers and other School ICT equipment/devices without obtaining prior consent from the student/Parent/Guardian. For example, teachers may at any time check student email or work.

8. ONLINE SAFETY

Students are given training regarding online safety practices. Parents/Guardians are encouraged to visit the websites below to become aware of the risks involved in using the internet and strategies for increasing safe use. Personal information is easily tracked and harvested by those who know how, so it is important that users keep as safe as possible whilst online.

Cyberbullying is now one of the leading forms of bullying. By monitoring how their child uses social media platforms such as Facebook and YouTube at home, Parents/Guardians can become active in minimising and preventing cyberbullying. Cyberbullying that occurs outside of school may still be subject to sanctions as outlined in the School's *Bullying and Harassment Policy*.

https://esafety.gov.au/ - the Australian Government's online safety information website with sections for parents and young people.

https://esafety.gov.au/education-resources/iparent/ - a subsection of the Australian Government's eSafetyCommissioner website specifically designed to help parents/guardians keep children safe in the digital world and manage ICT at home.

9. MANAGING THE DEVICE AT HOME

It is suggested that when used at home the Device should be in a shared or visible location so parents/guardians are aware of how much time is spent on the Device and the nature of what it is being used for.

Information on managing technology in the home, safety settings, parental controls, filtering software and online safety can be found at https://esafety.gov.au/education-resources/iparent.

PLEASE NOTE: Any questions about this document are to be referred, in the first instance, to the Finance Department.

APPENDIX A

INFORMATION COMMUNICATION TECHNOLOGIES APPROPRIATE USE POLICY: STUDENTS

PREAMBLE AND DEFINITION OF INFORMATION COMMUNICATION TECHNOLOGIES

John Wollaston Anglican Community School (the School) prides itself on providing educational experiences that are meaningful and relevant for all students. Digital technologies play an integral part in promoting this. The appropriate use of digital technologies has the potential to enhance student learning immensely. The School is aware that there are also dangers associated with such technologies, therefore the School has developed and implemented an *Information Communication Technologies (ICT) Appropriate Use Policy: Students* to address issues of online safety.

ICT covers a broad spectrum of equipment/devices including mobile phone technology. For the purposes of this policy, they refer to and include all forms of technology that are used at the School, inclusive of the Internet, School computer network, email, software, computers (laptops, tablets, smart phones, desktops, PDAs), storage devices (such as USB and flash memory drives, external drives, CDs and DVDs), video and audio players/recorders, gaming consoles and other similar technologies as they come into use.

GUIDELINES FOR APPROPRIATE USE BY STUDENTS

The guidelines below refer to the use of any devices/equipment, including that which is privately owned, BYOD, on the school site or at/for any school related activity, regardless of its location. This includes off-site use of student devices and any other school owned/leased ICT equipment/devices and access to the School network.

1. Students may only use the School's Internet and School-owned/leased devices/equipment if a signed copy of this *ICT Appropriate Use Policy: Students* has been returned to the School.
2. The use of the Internet and device/equipment is to be used only for educational purposes under the direction of School staff.
3. The following types of use or similar are prohibited and may result in School sanctions and/or Police involvement:
   - Sharing of usernames and passwords with other students or allowing another student to work on their account.
   - Violating or infringing the rights of any other person, including the right to privacy.
   - Initiating access to objectionable, inappropriate or illegal material.
   - Initiating access to material which contains actual or potentially defamatory, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually explicit, sexually oriented, threatening, racially offensive or otherwise biased, discriminatory, illegal or any other objectionable or inappropriate material.
   - Violating any other School Agreement, including prohibitions against harassment of any kind.
   - Placing images of a student or staff member on the Internet or the School's network without the person's permission.
   - Failing to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus.
   - Placing viruses, applications or similar on the School's network or other user's devices that are designed to interrupt, or imitate interruption to, normal operating processes.
   - Attempting to access personal data by using or attempting to use others' passwords with or without their permission.
   - Involving sharing of copyright material e.g. music, movies, games, applications or software.
   - Attempting to breach security and infrastructure that is in place to protect user safety and privacy.
   - Initiate network port and IP scans for any reason.
   - Obtaining unauthorised access to the School's electronic communication system.
   - Inhibiting the user's or another's ability to learn productively and without unnecessary interruption.
   - Involving the unauthorised installation and/or downloading of non-School endorsed software.
   - Offending or potentially offending the ethos, principles and/or foundations of the School.

- Involving malicious activity resulting in deliberate damage to School ICT and/or ICT equipment/devices.
- Bringing the School or members of the School community into disrepute.

4. In the event of accidental access of such material, users must:
   - Not show others.
   - Close or minimise the window.
   - Report the incident immediately to a member of staff.

MONITORING BY THE SCHOOL

The School reserves the right at any time to check work or data on:

- The School's computer network, Internet access facilities, computers and other school ICT equipment/devices without obtaining prior consent from the relevant authorised user. For example, teachers may at any time check a student's email or work.
- Privately-owned or leased ICT equipment on the school site or at any school-related activity, the authorised user agrees to promptly make the ICT equipment/device available to the School for the purposes of any such check and to otherwise co-operate with the School in the process. Before commencing the check, the School will inform the authorised user the purpose of the check.

The School has several electronic access monitoring systems which have the capability to record email and Internet use, including the user details, time, date, sites visited, length of time viewed and from which computer or device.

THE USE OF SOCIAL MEDIA

Students are not permitted to access any forms of social media content at school unless directed by staff for educational purposes.

ONLINE SAFETY

Online safety refers to the safe and responsible use of the Internet and any other digital form of sharing information such as, but not limited to, email and texting. Users need to pay particular attention to the information shared on the Internet including social networking sites such as Facebook and video sharing sites such as YouTube.

Students should not offer any personal information including last name, contact information, home address, telephone numbers, the School's name, e-mail address, last names of friends or relatives, instant messaging names, age, or birth date. Students are advised never to post provocative pictures of themselves or anyone else and be sure any images they provide do not reveal any of the previously mentioned information. Remember to also check the background of a picture. It should be assumed that anything posted online may be seen by anyone.

Students are given training regarding online safety practices and are expected to use ICT equipment/devices in a safe manner.

CYBERBULLYING

Students do not have access to social networking sites during school hours. Students who engage in antisocial behaviour on social networking or blogging sites that impacts the John Wollaston community, such as bullying a fellow student, will be subject to school sanctions and/or legal regulations regarding such behaviour even though the infringements occurred off campus. Students must not engage in bullying, spamming, illegal behaviour, malicious blogging or similar antisocial behaviours.

Laws that apply in the real world also apply online. Cyberbullies will be dealt with as outlined in the School's *Bullying and Harassment Policy*. Students who become knowledgeable of such practices are required to inform a member of School staff.

BREACHES OF THE APPROPRIATE USE GUIDELINES

Students who use ICT in an inappropriate manner will be given a sanction considered appropriate by the School. In serious matters the Police may also be involved.

Students who use ICT in an inappropriate manner may face sanctions including but not limited to:

- After school detention.
- A temporary or permanent ban on ICT use.
- Suspension.
- Exclusion.

RETAIN THIS COPY OF THE POLICY FOR YOUR RECORDS

John Wollaston
ANGLICAN COMMUNITY SCHOOL

APPENDIX B

STUDENT BYOD YEARS 10 to 12 USER AGREEMENT

Please read carefully through this document before signing the return copy.

By signing this form, you are agreeing to use your BYOD according to the stated guidelines. If you do not understand any part of the Agreement, please seek clarification from a Parent/Guardian or member of staff. Students who do not follow the guidelines may lose the privilege of using their Device at school and face other sanctions.

1. I have read the *ICT Appropriate Use Policy: Students* and will use my Device in accordance with this policy.

2. I understand that my Parents/Guardians are responsible for organising any repairs or a replacement in the case of damage or loss of my Device.

3. I will not decorate my Device with any sort of marking or sticker that is not in keeping with the School ethos.

4. When at school I will not use my Device during break times or if unsupervised by a teacher.

5. I acknowledge I am responsible for backing up and saving my data and that if my Device needs repairing, I may lose anything stored on the Device itself.

6. I will cooperate and make my Device available to School staff as requested to do so.

This is your copy of the Student BYOD Years 10 to 12 User Agreement.
PLEASE RETAIN THIS COPY FOR YOUR RECORDS.

APPENDIX C

INFORMATION COMMUNICATION TECHNOLOGIES APPROPRIATE USE POLICY: STUDENTS

PREAMBLE AND DEFINITION OF INFORMATION COMMUNICATION TECHNOLOGIES

John Wollaston Anglican Community School (the School) prides itself on providing educational experiences that are meaningful and relevant for all students. Digital technologies play an integral part in promoting this. The appropriate use of digital technologies has the potential to enhance student learning immensely. The School is aware that there are also dangers associated with such technologies, therefore the School has developed and implemented an *Information Communication Technologies (ICT) Appropriate Use Policy: Students* to address issues of online safety.

ICT covers a broad spectrum of equipment/devices including mobile phone technology. For the purposes of this policy, they refer to and include all forms of technology that are used at the School, inclusive of the Internet, School computer network, email, software, computers (laptops, tablets, smart phones, desktops, PDAs), storage devices (such as USB and flash memory drives, external drives, CDs and DVDs), video and audio players/recorders, gaming consoles and other similar technologies as they come into use.

GUIDELINES FOR APPROPRIATE USE BY STUDENTS

The guidelines below refer to the use of any devices/equipment, including that which is privately owned, BYOD, on the school site or at/for any school related activity, regardless of its location. This includes off-site use of student devices and any other school owned/leased ICT equipment/devices and access to the School network.

1. Students may only use the School's Internet and School-owned/leased devices/equipment if a signed copy of this *ICT Appropriate Use Policy: Students* has been returned to the School.
2. The use of the Internet and device/equipment is to be used only for educational purposes under the direction of School staff.
3. The following types of use or similar are prohibited and may result in School sanctions and/or Police involvement:
   - Sharing of usernames and passwords with other students or allowing another student to work on their account.
   - Violating or infringing the rights of any other person, including the right to privacy.
   - Initiating access to objectionable, inappropriate or illegal material.
   - Initiating access to material which contains actual or potentially defamatory, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually explicit, sexually oriented, threatening, racially offensive or otherwise biased, discriminatory, illegal or any other objectionable or inappropriate material.
   - Violating any other School Agreement, including prohibitions against harassment of any kind.
   - Placing images of a student or staff member on the Internet or the School's network without the person's permission.
   - Failing to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus.
   - Placing viruses, applications or similar on the School's network or other user's devices that are designed to interrupt, or imitate interruption to, normal operating processes.
   - Attempting to access personal data by using or attempting to use others' passwords with or without their permission.
   - Initiate network port and IP scans for any reason.
   - Involving sharing of copyright material e.g. music, movies, games, applications or software.
   - Attempting to breach security and infrastructure that is in place to protect user safety and privacy.
   - Obtaining unauthorised access to the School's electronic communication system.
   - Inhibiting the user's or another's ability to learn productively and without unnecessary interruption.
   - Involving the unauthorised installation and/or downloading of non-School endorsed software.
   - Offending or potentially offending the ethos, principles and/or foundations of the School.

- Involving malicious activity resulting in deliberate damage to School ICT and/or ICT equipment/devices.
- Bringing the School or members of the School community into disrepute.

4. In the event of accidental access of such material, users must:
   - Not show others.
   - Close or minimise the window.
   - Report the incident immediately to a member of staff.

MONITORING BY THE SCHOOL

The School reserves the right at any time to check work or data on:

- The School's computer network, Internet access facilities, computers and other school ICT equipment/devices without obtaining prior consent from the relevant authorised user. For example, teachers may at any time check a student's email or work.
- Privately-owned or leased ICT equipment on the school site or at any school-related activity, the authorised user agrees to promptly make the ICT equipment/device available to the School for the purposes of any such check and to otherwise co-operate with the School in the process. Before commencing the check, the School will inform the authorised user the purpose of the check.

The School has several electronic access monitoring systems which have the capability to record email and Internet use, including the user details, time, date, sites visited, length of time viewed and from which computer or device.

THE USE OF SOCIAL MEDIA

Students are not permitted to access any forms of social media content at school unless directed by staff for educational purposes.

ONLINE SAFETY

Online safety refers to the safe and responsible use of the Internet and any other digital form of sharing information such as, but not limited to, email and texting. Users need to pay particular attention to the information shared on the Internet including social networking sites such as Facebook and video sharing sites such as YouTube.

Students should not offer any personal information including last name, contact information, home address, telephone numbers, the School's name, e-mail address, last names of friends or relatives, instant messaging names, age, or birth date. Students are advised never to post provocative pictures of themselves or anyone else and be sure any images they provide do not reveal any of the previously mentioned information. Remember to also check the background of a picture. It should be assumed that anything posted online may be seen by anyone.

Students are given training regarding online safety practices and are expected to use ICT equipment/devices in a safe manner.

CYBERBULLYING

Students do not have access to social networking sites during school hours. Students who engage in antisocial behaviour on social networking or blogging sites that impacts the John Wollaston community, such as bullying a fellow student, will be subject to school sanctions and/or legal regulations regarding such behaviour even though the infringements occurred off campus. Students must not engage in bullying, spamming, illegal behaviour, malicious blogging or similar antisocial behaviours.

Laws that apply in the real world also apply online. Cyberbullies will be dealt with as outlined in the School's *Bullying and Harassment Policy*. Students who become knowledgeable of such practices are required to inform a member of School staff.

BREACHES OF THE APPROPRIATE USE GUIDELINES

Students who use ICT in an inappropriate manner will be given a sanction considered appropriate by the School. In serious matters the Police may also be involved.

Students who use ICT in an inappropriate manner may face sanctions including but not limited to:

- After school detention.
- A temporary or permanent ban on ICT use.
- Suspension.
- Exclusion.

I have read the *ICT Appropriate Use Policy: Students* and I will follow the terms of this agreement.

Student Name	**Student Signature**	**Date**
Parent / Guardian Name	**Parent / Guardian Signature**	**Date**

PLEASE RETURN THIS COPY TO STUDENT SERVICES RECEPTION

Submission of this form will be required before the device is distributed.

OFFICE USE ONLY

1. Student Services Reception

Student signed ☐ *Parent/Guardian signed* ☐ *Date* _____

Paperwork to IT ☐ *Date* _____

2. IT Department

Device issued ☐ *IT Department recorded* ☐

3. Administration

Scanned to student file and form placed on file ☐

John Wollaston
ANGLICAN COMMUNITY SCHOOL

APPENDIX D

STUDENT BYOD YEARS 10 to 12 USER AGREEMENT

Please read carefully through this document before signing the return copy.

By signing this form, you are agreeing to use your BYOD according to the stated guidelines. If you do not understand any part of the Agreement, please seek clarification from a Parent/Guardian or member of staff. Students who do not follow the guidelines may lose the privilege of using their Device at school and face other sanctions.

1. I have read the *ICT Appropriate Use Policy: Students* and will use my Device in accordance with this policy.
2. I understand that my Parents/Guardians are responsible for organising any repairs or a replacement in the case of damage or loss of my Device.
3. I will not decorate my Device with any sort of marking or sticker that is not in keeping with the School ethos.
4. When at school I will not use my Device during break times or if unsupervised by a teacher.
5. I acknowledge I am responsible for backing up and saving my data and that if my Device needs repairing, I may lose anything stored on the Device itself.
6. I will cooperate and make my Device available to School staff as requested to do so.

I have read the *Student BYOD Years 10 to 12 User Agreement* and I will follow the terms of this agreement.

Student Name	Student Signature	Date

Parent / Guardian Name	Parent / Guardian Signature	Date

PLEASE RETURN THIS COPY TO STUDENT SERVICES RECEPTION

Submission of this form will be required before the device is distributed.

OFFICE USE ONLY

1. Student Services Reception

Student signed ☐ *Parent/Guardian signed* ☐ *Date* _____

Paperwork to IT ☐ *Date* _____

2. IT Department

Device issued ☐ *IT Department recorded* ☐

3. Administration

Scanned to student file and form placed on file ☐