Catholic Education
Diocese of Rockhampton

2021 Information and Communications Technologies Code of Practice including Holy Spirit College Digital Assistant Program (DAPR) Guidelines

Student: Secondary Years 7 – 12

Version 6 • December 2021
Document Number: D17/31348[V6]
Date of next Review: 2022
Author: Administration

CONTENTS

1. Introduction

The purpose of Information and Communications Technologies (ICT) for students at Holy Spirit College, Mackay Qld, is to:

- enhance student learning opportunities
- promote student achievement
- support student – school communication

The use of ICT within the school should be safe, responsible, legal, appropriate and for educational purposes and should follow the guidelines outlined in this Code of Practice.

This Code of Practice applies to the use of all school related ICT whether provided by the school, employees of the school or the student.

Both students and parents/guardians must read and sign this Code of Practice. It should be returned to Holy Spirit College.

2. Definitions

The following words are commonly used within this Code of Practice and are defined as follows to assist you in reading this document:
"**Catholic Education**" means The Roman Catholic Trust Corporation for the Diocese of Rockhampton trading as Catholic Education Rockhampton. Catholic Education includes the Catholic Education Diocese of Rockhampton (CEO), Catholic systemic schools, services and work sites of Catholic Education.

"**Student**" means persons enrolled within a Catholic Education college within the Diocese of Rockhampton.

"**Information and Communications Technologies**" (ICT) means any electronic devices or services which allow users to record, send or receive information, in audio, text, image or video form. These devices or services may include but are not restricted to standalone and networked:

- computer systems and related applications such as email and internet;
- social media;
- mobile devices including wearable technologies;
- communication equipment;
- output devices such as printers;
- imaging tools such as video or still cameras;
- audio tools such as audio recording devices;
- software applications and externally provided electronic services.

"**Social media**" means websites and applications and any other service or device which enable a user to create and share content or to participate in social networking. This includes but is not limited to Facebook, LinkedIn, Instagram, Snapchat, Pinterest, Twitter, blogs, forums, discussion boards, chat rooms, wikis and YouTube.

3. Acceptable Uses

3.1. Students should:

- Respect resources
- Use ICT equipment and resources for educational purposes independently and under adult supervision
- Access files, programs, email and internet resources appropriately
- Respect self and others by:
  - Respecting the rights, beliefs and viewpoints of others
  - Following the same standards of behaviour online as one is expected to follow offline
  - Observing copyright rules by respecting the information, ideas and artistic works of others by acknowledging the author or publisher of information from the internet and not claiming the work or pictures as your own
- Keep safe by:
  - Ensuring passwords and personal work are secure. If it is suspected that a password has been compromised, steps must be taken to change the password immediately.
  - Using school email accounts, not personal accounts, when communicating for educational purposes
  - Using social media appropriately including abiding by the application's terms and conditions
  - embracing the principles of good digital citizenship

4. Unacceptable Uses

4.1. Personal Safety

Disclosure of personal information can expose users to inappropriate material, physical danger, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance and sabotage.

You should NOT:

- Send or post detailed personal information, images or audio about yourself or other people. Personal contact information includes your full name, date of birth / age, home address, telephone or mobile number, school address or work address.
- Publish email addresses to public sites
- Access personal mobile phones or wearable technology during school hours

4.2. Respect for Privacy

You should NOT:

- Distribute private information, including email, photos or recordings, about another person without their permission
- Take photos, sound or video recordings of people, including background figures and voices, without their permission

4.3. Respect for Others

You should NOT:

- Make personal attacks including harassing and bullying another person. If someone tells you to stop sending them messages, you must comply with their request.
- Send or post any inappropriate or inaccurate information, comments, images, video or audio about other people, the school or other organisations.
- Send or post personal information about other people without their permission.

4.4. Inappropriate Language

Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages.

Messages sent using the school's ICT are recorded, monitored and scanned.

You should NOT:

- Use obscene, profane, rude, threatening, sexist, racist, disrespectful or inappropriate language.

4.5. Access to Inappropriate Material

Attempts to access inappropriate material using the school's ICT is monitored and logged by the school or the Catholic Education Office.

Some inappropriate material may be filtered or blocked by the school or Catholic Education Office.

You should NOT:

- Use ICT to access material that:
  - is profane or obscene (e.g. pornography);
  - advocates illegal acts;
  - advocates violence or discrimination towards other people;
- Participate in internet social networks, online chats, discussion groups or mailing lists that are not relevant to your education.
- Access material which is not relevant to your education.
- Use the school ICT to purchase, order or sell any goods.

4.6. Illegal Activities

Students need to be aware that they are subject to laws which prohibit posting, receiving or forwarding of illegal material, including those governing bullying, trafficking and computer offences.

An electronic audit trail may provide evidence of offences.

You should NOT

- Attempt to gain access to any computer system or service, to which you do not have authorised access. This includes attempting to log in through another person's account or accessing another person's files or emails.

- Make deliberate attempts to disrupt other people's use of ICT.
- Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.
- Engage in any illegal acts.
- Install or use software on school owned devices which is not authorised by the school.

4.7. Plagiarism and Copyright

You should NOT:

- Plagiarise works found on the internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Use material from the internet in a manner which violates copyright laws
- Access or use material from the internet which relates to exam cheating or providing completed assignments.

4.8. Network Security

You should NOT:

- Provide your password to another person.
- Go looking for network security access, because this may be seen as an attempt to gain unauthorised access to the network.
- Post information that, if acted upon, could cause damage to or disrupt the network.
- Open e-mails from unknown sources.
- Install or utilise software or technology e.g. hotspots which bypasses the school or CEO filters or security systems.

4.9. Respecting Resource Limits

You should NOT:

- Post or respond to chain letters or engage in 'spamming'. Spamming is sending an annoying or unnecessary message to a large number of people.

5. Notification

You should:

- Report inappropriate communications using the application's reporting mechanisms.
- Notify your teacher or carer if you identify a possible security problem.
- Immediately disclose accidental access to inappropriate material to your teacher. This will protect you against an allegation that you have intentionally violated the School's ICT Code of Practice.
- Notify your teacher if you are offended by another person's use of ICT.
- Tell a teacher or parent/guardian if someone else is doing something which offends you or is not permitted.

6. Consequences of Improper Use

Minor breaches of the ICT Code of Practice will be addressed by the relevant Holy Spirit College staff member in line with Holy Spirit College's behaviour management procedures. If deemed appropriate, the student's account may be suspended.

Ongoing or serious breaches of the ICT Code of Practice may result in further consequences, including suspension and / or exclusion from the college.

Please note, all schools and colleges in the Diocese of Rockhampton are legally required to pass on information to police relating to the possession, distribution or production of child sexual abuse material, images or video of themselves or their peers, including that which has been taken or shared consensually. The outcome of the investigation conducted by police will impact the consequences to the student/s by the college.

In summary, any user violation will be recorded and may be subject to the following consequences:

- loss of access privileges for a period of time;
- informing parents/guardians;
- suspension or termination of enrolment;
- legal action;

7. Cloud Services for Education – Advice for Parents

All students have access to educational collaborative Virtual Learning Environments (VLE) which include Google G-Suite for Education and Microsoft Office 365. These environments provide access to email and a range of collaborative and productivity tools.

In using the Virtual Learning Environments provided through CEnet and the Rockhampton Catholic Education Diocese, students (with parent permission) consent to the transfer, processing and storage of their data within cloud services.

The CEnet Agreement with Google and Microsoft and the actions taken by Dioceses to establish ICT Codes of Practice will ensure the protection of personal information in accordance with national privacy, data usage, and data security guidelines.

- All advertising is disabled for education users to ensure that there is no tracking of school emails or web browsing.
- All mail is automatically scanned to perform spam filtering, virus detection and to block inappropriate content.
- Authorised staff within Catholic Education will have the ability to access, monitor, and audit emails and associated data as well as internet sites visited for the purposes of managing the system and ensuring its proper use.

8. Holy Spirit College - Digital Assistant Program (DAPR) Guidelines

8.1. Vision Statement

HSC is excited that students at Holy Spirit College have their own 'digital assistant' to support their secondary education! Online resources provide a wealth of teaching tools to enhance our learning programs.

Our students use their 'digital assistant' to:

- learn 'anywhere, anytime'.
- use the largest and most up-to-date library ever available in the world's history.
- access information instantly at their desk without needing to be scheduled into computer rooms.
- access 'digital textbooks' and resources developed by our teachers which provide so much more than a standard textbook – videos, animations, documents, tutorials and live interviews, face to face conversations with classes in other countries, with new possibilities developing constantly.
- access information quickly so there is more time for deeper understanding, analysing and connecting ideas.
- work ahead or revisit online learning for more practice.
- organise their work for class and assignments.
- find learning more interesting and become more motivated and self-directed.
- be able to complete their school work without competing with other members of the family for computer use.
- continually develop proficiency with computers for living and working in a digital world.
- understand how to be safe in the online world through Cybersafety training.

DAPR (The HSC Computer program) does not:

- replace handwriting, spelling, English and Mathematical skills, exercise books and Libraries.
- replace our traditional ways of teaching and learning but add many new dimensions.
- allow students to just copy their assignments from the Internet but teaches them to collate information from many sources into their own conclusions.

8.2. Using your Digital Assistant

Students are to bring their computer to school each day.
During Pastoral Care, teachers check that students have brought their computer to school and parents are notified through the Student Diary if students fail to do so. Teachers may request that Students make up work that was not completed due to the absence of their computer.

Holy Spirit College provides students with an internet accessible Learning Management System (LMS) called Student Café, and Google Classroom and OneNote also supplement the LMS. Teachers provide subject resources to students such as: assignment cover sheets, worksheets, revision, links to online resources, research information and documents, online submission of checkpoints and final assignments, updates on completion of assignments and due dates, class discussion forums and blogs, and online tests. Student Café also provides access to student daily and weekly timetables, daily notices, attendance and links to the student webmail system.

Students can expect to use their computer on average for 2 to 3 lessons in the 5 lesson day. In addition to their core subjects, students study subjects whose practical basis requires students to be away from desks and developing other skills. Core and appropriate elective subjects have learning programs which incorporate digital learning.

Students will still be required to produce handwritten work and use printed texts and novels. The Digital Assistant enables teachers to bring to life those parts of the curriculum which are enhanced and extended by digital learning.

Privately installed software

Students are able to add any software they wish to their computer as long as it remains within copyright, licensing and the College's ICT Code of Practice and DAPR Guidelines. If the addition of software to DAPR package computers (Option A) causes conflicts with other installed programs, and results in impaired performance or does not leave sufficient space for school work to be done, the DAPR package computer may need to be reimaged at the HelpDesk (resetting the computer back to its original contents) to allow for successful operation. Option B computer may need to be reimaged using the functions of the computer purchased.

Battery

Students will need to make sure that their computer battery is fully charged for school each day. They will need to ensure that their device is on charge overnight if needed so that it is fully operational for the day. Students should ensure they have sufficient battery charge to last until the end of the day if they choose to use their laptop during recesses.

The DAPR package computer (Option A) is equipped with a battery to provide extended daily usage. Some suggestions provided by HP to care for the HP battery can be found in Appendix D.

Backpacks

Students now have an additional item to be stored in their backpack or to be carried separately. Please examine the contents of your student's backpack to check they are only bringing the books for the current day, all unnecessary items are left at home and the size of essential items is as small as possible.

HelpDesk for students using Option A (DAPR package computers)

Should a student experience difficulty with the operation of their DAPR package computer they should visit the HelpDesk in Room 12 to report the problem.

The HelpDesk is open for students between 8:30am and 2:15pm on school days. During class time the Helpdesk can only be accessed by students if a teacher has directed a student to do so, and the teacher has called the Helpdesk first to make sure there is someone available to assist. Students will need to bring their Student Diary with them when visiting the HelpDesk.

The HelpDesk will assess the problem. The following steps may be taken:

- Minor problems will be attended to by the HelpDesk Assistant where possible.
- Software problem – Computer will be booked in for reimaging to the original setup to eliminate problems so the student can resume use. All contents of the computer will be erased in the re-imaging process. Students will need to backup all their work and reinstall.
- Warranty problem – where the computer appears to have a hardware problem which is covered by warranty, the computer will be registered for warranty repair (within the warranty period). Students will be notified when the computer is ready for pickup. The College has a small stock of computers which may be loaned to a student awaiting a warranty repair. Any damage to loaned computers will need to be repaired at the student's expense and conditions of use will need to be agreed to prior to use of a loaned computer.
- Accidental Damage Protection (ADP) is included with the HP Notebook package. Students are covered for 3 major component replacements due to accidental damage per year (a $60.50 HP excess is payable per claim). Students presenting damaged computers to the HelpDesk for repair will be asked to complete a form outlining the circumstances in which the damage occurred. This form will need to be returned to the HelpDesk signed by Parents and the HP ADP excess paid to Holy Spirit College Finance Office before repairs can be arranged. (Details of the Damage Reporting Process for ADP is outlined in Appendix A.) In the event of malicious damage or theft – an Insurance Claim will need to be considered by the family in accordance with their insurer's requirements. Families may wish to consider insurance for the student device without the cover of an ADP.
- The College HelpDesk is not available during school holidays. Computers under warranty can be registered for HP repair by parents, if required, during holidays by calling 131047.

HelpDesk for students using Option B (Bring Your Own Device – BYOD)

The HelpDesk assists students to make connection to the College's wireless network. Logins and Passwords are supplied to students so they can access licensed online learning. Basic software requirements, as listed on the DAPR Options Form, will need to be available on the computer for student use in class and supplied and maintained by the family.

Students who have problems with their device can bring it to the HelpDesk for advice. While we do not repair BYOD (Option B) computers, the HelpDesk may be able to give advice on the next step to solving the problem.

The HelpDesk does not have a reimage capacity for computers other than the current DAPR package computer models so will be unable to assist with reimaging. Parents will need to seek an external repair service or make a warranty or insurance claim as required according to the agreements made with their vendor.

At Home

Holy Spirit College provides external access to the College Learning Management System (Student Café) to allow students access to these resources from home. Students may also require external access to other online resources provided by subject teachers for their classes to use such as Google Classroom, Box of Books, Maths Online and Education Perfect. An Internet connection at home will allow students to access this material whenever they wish. Students are welcome to install their home wireless network on their DAPR or BYOD Computer for use at home without deleting the Holy Spirit College wireless network settings.

Holy Spirit College is committed to equity for all students. If the Internet is not available at home then students will be able to access the Internet in the Library until 4pm after school each day. Alternative paper based work will be available if needed. Students also have the option of copying documents to their computer at school to be used at home. Please let the subject teacher know if there are particular requirements.

Printing

As digital learning continues to develop, the necessity for printing reduces. Where students need to print, the Library is open until 4pm each day and a Computer Lab (as needed) will be open at first break for black and white printing only. Students can use a USB memory stick for printing in the Library. Printing is a resource which needs to be used by students in a responsible manner and with respect for all other users. Research printing should abide by copyright guidelines and be economical by cutting and pasting essential content only. Printing costs 10c per page.

Printing at home is also an efficient method for students to obtain hard copies. Families are welcome to install printer drivers for the home printer on their student's computer.

Computer usage during lunch breaks

The College has a wireless network which is accessible to the majority of the classrooms and grounds during teaching lessons. DAPR students will have access to the wireless network in lunch breaks. They are welcome to use their computer in the Tutorial rooms and Reading areas of the Library which are supervised by teaching staff.

Backup Responsibility

Students are responsible for 'backing up' all their work including group work. Saving work on to the hard drive of their computer is not sufficient protection against loss. Loss of work due to equipment failure is not accepted as a reason for not submitting assessment on time. Students will need to have at least one backup device (two are recommended) and to backup on a regular schedule e.g. fortnightly to very frequently when large volumes of work are being done.

A USB stick is valuable for ease of transport and accessing printing at school if required. This device can be used to store (or backup) student files but a USB is not sufficient protection against lost work. Students may find other alternatives for larger storage such as an external hard drive, which also gives extra security against loss of valuable work. Emailing work to their own account is another way to backup if other methods are not available although this will be dependent on the size of the storage available for the email account. It is good practice to save throughout a work session. HSC also recommends students utilise Google Drive for automatic saving in the cloud.

Where significant progress has been made on an assignment involving larger volumes of text a printed copy at important stages is also a valuable backup. A printed copy of partial-completion can be submitted as evidence of progress.

Earphones
To ensure a productive working environment for all students, sound will be muted at all times and earphones are to be used whenever a teacher directs students to listen to audio files on their computer. Students should have a set of earphones in their pencil case.

Managing Files
It will be to the student's advantage not to waste valuable learning time in class searching for files in their hard drive. A hierarchy of folders needs to be created by all students with levels for subjects and terms or topics so that work can be stored and located efficiently. Files should be clearly named and additional folders created as required.

Personalising your computer
Students are welcome to personalise their desktop and screensavers within the requirements of the ICT Code of Practice and DAPR Guidelines to maintain appropriate standards for a Catholic Educational Community.

Security and Care of the Computer
Students are responsible for the safety of the computer at all times. They should always know where it is and must not leave it unattended. While the College institutes guidelines and procedures to protect all private and College-owned items, the College cannot accept liability for the security of students' possessions. The student is responsible for any material on or transmitted from their computer so they must not leave it available for other students to use or tamper with. Further information on the care of the computer can be found in Appendix C.

'Screens Down' Instruction
Similar to the 'pencils down' instruction of previous generations, the 'screens down' instruction will be given to students during lessons as they move from digital activities to paper-based, practical, group work or teacher instruction activities. Students are to comply promptly.

Internet safety
The College Internet service provides a level of filtering which is used by many Catholic Colleges throughout Australia. Every effort is made by the filtering service to ensure that unsuitable material is not accessed by students; however, this is not an absolute guarantee. Staff at Holy Spirit College provide supervision when the Internet is in use by students to add another layer of protection. Ultimately there is no perfect protection and students are responsible for managing their Internet usage. Anything they view that causes them concern should be reported to their teacher and students should follow cybersafe practices – refer Appendix B.

Students using the Internet at home are under the protection of their parents. Commercially available software can provide some protection. Supervision by parents is an invaluable support for students. Students should only be accessing the Internet through their HSC login which provides a monitored service and not through alternative access. Using an alternative internet access is a breach of the ICT Code of Practice and DAPR Guidelines and consequences will apply.

Students must not agree to meet with someone they have met online.

On task learning
Students are to remain on task with the use of their computer and Internet access. Electronic communication with others in the College grounds or in the outside community is prohibited unless directed by a teacher through a learning activity.

Monitoring Computer Use
All student computers used at Holy Spirit College are monitored by teachers using a licensed software package called LanSchool. Option A student notebooks are provided with this program installed and Option B student notebooks have LanSchool installed at the College. Internet access at the College is also monitored and all student Internet use is logged and tracked.

DAPR Staff

IT Helpdesk Assistant	Tanya Bridson
IT Manager	Brendan Field

IT HelpDesk open 8:30am-2:15pm daily / Ph: 4994 8600 / Email DAPR@hsc.qld.edu.au

8.3. Approved Use

Scope
These guidelines apply to all student-owned computers, hardware and software used at Holy Spirit College. It includes computers purchased outright through the College, privately purchased computers irrespective of ownership and any other peripherals that are considered by the IT Manager to come under this agreement. It applies to all Holy Spirit College IT resources regardless of how they are accessed and including access through all College and user-owned devices, whether wired or wireless or remotely accessed over the Internet through the user's own resources.

These guidelines can never anticipate all possible advances and uses of technology and therefore students who are unsure about their usage should seek clarification from a teacher as soon as possible. If a student acts in a way that is against the contents and intention of the guidelines, he or she will be subject to consequences according to the College's policies. This may also result in loss of access to the College's IT services and the student working by other means. If necessary, offending material may be supplied to external authorities.

Privacy of Private Devices

Users may install software onto their owned devices but this software must not contravene the ICT Code of Practice and DAPR Guidelines or any other policies of the College regarding the legality, suitability and appropriateness of the software for the educational environment for which the computers are intended.

While user-owned computers are the personal property of the student, all computers used within the College Network environment will have classroom monitoring software installed. Holy Spirit College reserves the right to regularly monitor student computer use, and to look at a student's computer hard drive or other storage devices used at school if there is reasonable suspicion that the computer is being used for an inappropriate or dishonourable purpose. When a computer is handed in to the HelpDesk for support all information is accessible to the IT staff and external repair technicians.

IT Staff are responsible for the operation and maintenance of the IT systems and wireless network and this often requires backup and caching of data and monitoring online actions including logging website access, news-groups access, protocol, bandwidth and monitoring of general usage patterns so complete confidentiality and privacy is not guaranteed.

Appropriate Content

Information disseminated via the College's IT services is a reflection of how the global community perceives the College. All students using the services are encouraged to show that they are positive ambassadors for Holy Spirit College and themselves. No obscene, inflammatory, racist, discriminatory or derogatory language should be used in any form of communication.

Audio recording, photography and videoing functions

The use of live audio recording, photography and videoing functions on any device without the permission of the person being recorded and the instruction of the teacher is an unacceptable use of the device.

Copyright

The College is committed to total compliance with all copyright and related legal conventions. Holy Spirit College is the sole licensee of any licensed software supplied to students. Any copying, modification, merging, or distribution of the software by the student, including written documentation is prohibited.

Students must comply with all applicable laws and regulations.
The rights of copyright owners should be respected. Permission should be requested from the copyright owner where there is uncertainty over rights to use a work.

System Resources

Internet usage, printing and network storage are limited resources and should not be wasted. Students are required to use these valuable resources appropriately and with respect for other system users and their rights to share in these resources. Students who undertake excessive or inappropriate usage may be required to pay for this usage or may not be provided with access.

The network has been established for educational purposes including classroom activities, career development and high-quality self-discovery activities. These activities must be carried out according to the directions given by Holy Spirit College staff. Students should only use software specified by their teacher for activities specified by their teacher.

Use of unauthorised programs or intentionally downloaded unauthorised software, graphics or music that are not associated with the learning activity as directed by a staff member is prohibited. Students should never knowingly distribute spam, eg unsolicited advertising material or a computer virus or attachment that is capable of damaging recipients' computers, or disable settings for virus protection, spam and filtering that have been applied by the school and not attempt to evade them through use of proxy sites.

Student use of the Holy Spirit College network must not conflict with Catholic ethos, any part of the ICT Code of Practice or other College guidelines and policies.

Students may not enter computer rooms unless a teacher is present. No food, drink or gum (or any other substance or activity that is likely to damage school property or the rights of other College members) is allowed in the computer rooms or adjacent to computers.

Limitation of Liability

The College makes no guarantee that the functions or the services provided by or through the College system will be error-free or without defect. The College will not be responsible for any damage suffered, including but not limited to, loss of data or interruptions of service. The College is not responsible for financial obligations arising from the unauthorised use of the network and accepts no responsibility for the contents of sites accessed through links on the College website. The College accepts no responsibility for damage to student laptops.

Consequences

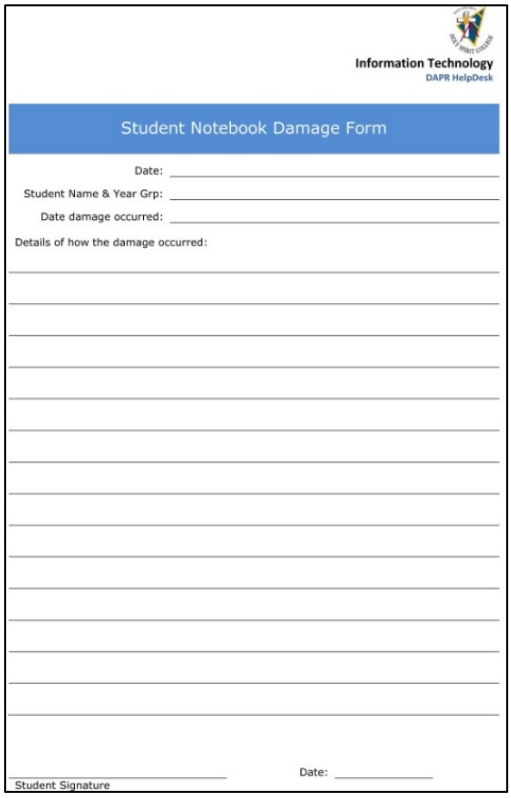
Breaches of the ICT Code of Practice will be managed through the Responsible Thinking Process. It is expected that damages will be paid for in full should a student mistreat school-owned equipment.

Appendix A

DAPR 'Option A' Students – Reporting Damage for Accidental Damage Protection (ADP)

Option A student notebooks are equipped with Accidental Damage Protection (ADP) which allows for 3 major component replacements, due to accidental damage, per year for the 3 years of the warranty period. (An accident to a computer may involve the replacement of more than 1 major component.) An excess of $60.50 is payable to HP per accidental damage claim and must be paid prior to the repair job being lodged. (A loan computer can be issued to the student on receipt of payment.)
The following outlines the steps required for reporting physical damage to Option A notebook computers:

- Student presents their damaged notebook to the IT HelpDesk in Room 12.
- Student will be asked to complete a "Student Notebook Damage Form".

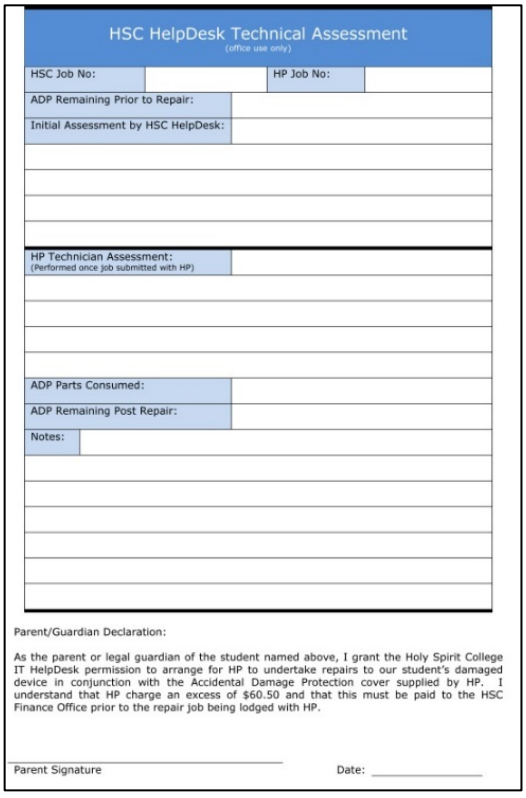


Information Technology
DAPR HelpDesk

Student Notebook Damage Form

Date: _____
Student Name & Year Grp: _____
Date damage occurred: _____
Details of how the damage occurred:

Student Signature _____ Date: _____



HSC HelpDesk Technical Assessment
(office use only)

HSC Job No:		HP Job No:	
ADP Remaining Prior to Repair:			
Initial Assessment by HSC HelpDesk:			
HP Technician Assessment: (Performed once job submitted with HP)			
ADP Parts Consumed:			
ADP Remaining Post Repair:			
Notes:			

Parent/Guardian Declaration:

As the parent or legal guardian of the student named above, I grant the Holy Spirit College IT HelpDesk permission to arrange for HP to undertake repairs to our student's damaged device in conjunction with the Accidental Damage Protection cover supplied by HP. I understand that HP charge an excess of $60.50 and that this must be paid to the HSC Finance Office prior to the repair job being lodged with HP.

Parent Signature _____ Date: _____

- Student takes the "Student Notebook Damage Form" home (with their damaged computer) for parent/guardian to view and sign.
- Parent/Guardian pays the required HP ADP Excess of $60.50 to Holy Spirit College Finance Office.
- Once the HP ADP Excess is paid, the student returns the signed "Student Notebook Damage Form" with the damaged notebook to the IT HelpDesk so that a job can be lodged with HP for repair.
- Once HP has completed repairs, details regarding the repair including how many Accidental Damage Protection (ADP) components were consumed, will be emailed to parents for their records.

NB: If you wish to pay the HP ADP Excess by cheque, please make it out to Holy Spirit College.

Appendix B

Cybersafety

The following guidelines comprise a list of behaviours which provide a safer online environment for students.

When using the school devices and services students will:

- ensure that communication through Internet and email services is related to learning.
- keep passwords confidential, and change them when prompted or when known by another user.
- use passwords that are not obvious or easily guessed.
- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- keep personal information including names, addresses, photographs, credit card details and telephone numbers, of themselves or others, private.

When using the school services or personal mobile phones (or similar personal equipment) students will not:

- allow others to use their personal accounts.
- deliberately use the electronic identity of another person to send messages to others or for any other purposes.
- enter 'chat' or 'social networking' Internet sites without the permission of a teacher.
- take photos or video of members of the school community without their consent.
- relay a message that was sent to them in confidence.
- send chain letters and hoax emails.

This section addresses the particular use of these technologies that has come to be referred to as Cyberbullying.
Cyberbullying will be taken and dealt with very seriously at Holy Spirit College. The school will investigate and take appropriate action where this kind of bullying occurs. Parents can also seek advice and assistance where Cyberbullying takes place outside of school hours. Consequences include, but are not limited to: investigation, mediation, suspension, and parent and police involvement. Students should be aware that if they use technology in an inappropriate fashion they could be committing a crime. Numerous state and commonwealth laws cover cyber crime.
When using school services or non-school services students will never send or publish either through Internet sites, e-mail or mobile phone messages:

- unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- threatening, bullying or harassing material or make unreasonable demands.
- sexually explicit or sexually suggestive material or correspondence.
- false or defamatory information about a person or organisation.
- the school name or crest without the written permission of the Principal.

Students need to be aware that all use of Internet and email services are monitored.

Appendix C

Care of Computer

Handling your computer

- The computer should be within the protective case when being transported.
- Never carry the computer while the screen is open, unless directed to do so by a teacher.
- Some carrying cases can hold other objects but these may add extra pressure and weight on the computer screen and damage it.
- The computer may be hibernated while not in use for short periods but should be shut down at the end of day for transportation.
- Do not lean on the top of the computer when it is closed.
- Do not place anything near the computer that could put pressure on the screen.
- Do not bump the computer against lockers, walls, car doors, floors as it will in time break the screen even when it is in its bag.
- Ensure all your computer components are named.
- Never leave the computer unsupervised.
- The bag should be fully zipped up before being carried.
- Unzip the bag fully before taking out the computer to avoid damage.
- Avoid exposing your computer to:
  - direct sunlight or sources of heat such as desk lamps
  - dust, dirt, rain, liquids or moisture
  - heavy shock or vibration

Operating your computer

- Before switching on, gently place your computer on a stable surface and then switch on.
- Do not use the computer in a moving vehicle.
- Avoid installing another virus protection program which may conflict with the current version.
- No food or drink should be allowed next to your computer

Computer screens

- Screens are very delicate - never poke, prod, push or slam a screen.
- Never pick up your computer by its screen.
- Never apply water or cleaner to the screen.
- Avoid applying pressure to the screen.
- Do not place anything on the keyboard before closing the lid eg pens, pencils, USBs

AC adapter

- Connect your adapter only to your computer.
- 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 the cord too tightly around the power adapter or the chord will become damaged.

Keyboard

- Gently brush your keyboard with a clean soft bristled paint brush or similar to remove dirt.

Appendix D

Care of Battery

Improving battery runtime – HP support advice

If you want to enjoy mobile use of your computer, and hence have as many minutes as possible while running on battery, here are a few tips which can help you improve the time your notebook can work on every single charge.

In order to improve the runtime of your battery, you can apply some or all of the below options:

- Disable wireless communications when not in use. Please check your user manual on how to disable Wireless LAN and Bluetooth on your model.
- Minimize the screen brightness of the built-in LCD panel to the minimum value you feel comfortable with. The lower you set your brightness, the less power you will use.
- Use an optimized power plan; all modern Operating Systems offer several options to optimize the power usage of your system when you are not using it for a short period of time. Hibernation or Standby Mode will allow the computer to use minimum power while you are away and to resume operation quickly when you are ready to use it again. Use the Power Options to configure the laptop to go inactive after a period of time.
- Try to avoid running heavy tasks, such as video editing or playing 3D games, on battery power. If you do, save your progress regularly to avoid losing work, since battery runtime will be highly impacted.

Note: all batteries lose capacity over time. While these tips can help improve the runtime, they will not reverse the effect of aging on a battery. It is normal behaviour for a battery to lose capacity over time, and is not a sign of failure.

It is not necessary to remove the battery when using AC power since the notebook provides a "trickle charge" to the battery while on AC. Some suggestions from HP on how to get the most life out of your notebook's battery are contained on the following URL - https://support.hp.com/us-en/document/c01297640 .

Other useful tips

- If you have multiple applications open at the same time close the ones you are not using. Every application that is running will drain the battery.
- Connecting other devices that require power from the computer will drain the battery.
- Avoid extreme temperatures, do not leave a laptop outside in the cold weather or leave it in a hot car. Hot batteries discharge very quickly, and cold ones can't create as much power.
- Decrease or mute the Laptop Speaker Volume.

Information and Communications Technologies Code of Practice

Letter of Agreement

Student

I understand and will abide by this ICT Code of Practice. I further understand that any violation of the above is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked and disciplinary and/or legal action may be taken.

Name (Please Print): _____

Signature: _____ Date: _____

Parent or Guardian

As the parent or guardian of this student, I have read the ICT Code of Practice. I understand that these resources are designed for educational purposes. I also recognise that it is impossible to completely restrict access to controversial material.

I hereby give permission for my child to be given access to information and communication technologies as deemed appropriate by the school. I am also aware that ICT Cloud service providers used by the Diocese may transfer, store and process data outside Australia.

Name (Please Print): _____

Signature: _____ Date: _____

NOTE: Failure to sign and return this agreement to your school will result in loss of access to ICT.