GLASSHOUSE
CHRISTIAN COLLEGE

MACBOOK PROGRAM STUDENT HANDBOOK

MIDDLE & SENIOR SCHOOLS

LAST UPDATED: 1 June 2017

Growing in faith and knowledge

TABLE OF CONTENTS

- MacBook Program Student Handbook
  - Table of Contents
  - The Principal's Address
  - Contact Details
- Daily Use and Care of your MacBook
  - Battery Charging and Care
  - Software Updates
  - Library Loans
  - Repairs and Replacement
  - Managing your Files and Saving your work
  - Regular Backups
- Safe Use of Technology
  - Social Media
  - Safety Tips for Students
  - Proxy Sites
  - Identity Theft
  - Australian Online Safety Links
  - Internet and Privacy
  - How we use Cookies
  - Cyberbullying
  - Monitoring at School
  - Monitoring at Home
  - MacBook Inspection
- Safe use of Technology - Physical Aspects
  - Stress Relief
  - Travelling With a MacBook
- Acceptable Usage for Students
  - Online Communication
  - Access and Security
  - Privacy and Confidentiality
  - Intellectual Property and Copyright
  - Misuse and Breaches of Acceptable Usage
  - Monitoring, evaluation and reporting requirements
  - Monitoring of communications

THE PRINCIPAL'S ADDRESS

The purpose of this handbook is to encourage the safe use of technology in our school and to clarify all the terms, conditions and responsibilities associated with the MacBook program options for all students in Year 7 to 12 who will be issued a 13' MacBook Air.

We believe the MacBook program has been of great benefit to our students both for learning and in preparation for the demands of the 21st century.

Mike Curtis
Principal

CONTACT DETAILS

For all Technical Information and Support please refer to Mr Roland Munyard
roland.munyard@glasshouse.qld.edu.au

For all Administrative and Policy related issues please speak with Administration
admin@glasshouse.qld.edu.au

DAILY USE AND CARE OF YOUR MACBOOK

Safe Use and Handling of your MacBook: You are expected to take full responsibility for securing your MacBook both on and off campus. MacBooks which are lost, damaged or stolen whilst in your care are your responsibility.

By using common sense and following this basic handling guidelines, you will get the most use and enjoyment out of your MacBook.

- Students are required to secure their MacBook with a login and password. Students are responsible for keeping their passwords secure
- All damages must be reported immediately to IT Services.
- If the MacBook is stolen the theft must be reported to the IT department immediately.
- Dropping your bag with the MacBook inside may cause severe damage to the computer.
- Do not drop your MacBook onto any hard surface (such as a desktop in the classroom) since damage can occur from even the slightest drop.
- Do not force your MacBook into tightly packed suitcases, bags or backpacks. The compression may cause damage to the MacBook or crack the LCD screen.
- The LCD screen must only be cleaned using a lint free cloth and approved LCD cleaner (kits are available from most computer suppliers). WARNING: Household cleaners may cause irreparable damage to the LCD screen.
- The case and lid may be cleaned using a clean dampened cloth that has had all excess water squeezed out. Do not place heavy objects on your MacBook screen.
- Do not allow drinks or liquids near your MacBook.
- Do not attempt to disassemble or alter any part of the MacBook. All repairs must only be performed by technicians authorised by IT Services.
- Do not scratch, dent or bend any part of the MacBook.
- The marking of your MacBook with stickers, pens, pencils or highlighters will be considered intentional damage. If your MacBook has graffiti of any type anywhere on the MacBook, you will be expected to pay for the required repairs.
- Do not place any objects between the keyboard and LCD screen,
- Do not pick up or hold your MacBook by the LCD screen.
- Do not store your MacBook where the temperatures fall below 5°C or above 35°C (41°F and 95°F).
- Do not leave your MacBook unattended at any time. All MacBooks must be kept secured either with you or locked in your locker. MacBooks are not to be left at the College after hours.
- You are not permitted to add stickers to your MacBook or mark it in any way.
- Only use the AC adaptor supplied with the MacBook. Do not attempt to use a different brand or model for charging your MacBook. Doing so may result in damage.
- It is essential that you fully charge your MacBook each night at home so it is ready for College the next day.

If the damage is not reported, but rather discovered by the IT department, the damage will be deemed to be mischievous or wilful. It is the responsibility of the student to report all damage.

The MacBook is a tool to support student learning at school and at home. The MacBook is intended for the sole use of the student it is issued to. While at College the computer will be used for school purposes.

For safety and security reasons, it is advisable that the MacBook not be used while in transit to or from school. MacBooks should be transported concealed within your school bag for the duration of your trip.

The LED screen is made of glass and is susceptible to damage. You should not push the screen with your finger or any object. Pressure on the screen may cause the screen to crack/fracture rendering the MacBook unusable. The LED screen should not be twisted or bent as this will also cause the screen to crack.

BATTERY CHARGING AND CARE

MacBooks must be fully charged in readiness for each school day. Students need to charge their MacBooks each evening. MacBooks will not be allowed to be charged at the College. Repeat violations of this policy will result in disciplinary action. Power chargers should be left at home.

The MacBook must only be charged with the Apple AC adaptor provided. A fully charged MacBook is essential for your ability to engage in learning activities for the day. To prolong the battery life it is recommended to keep the charger on at home when in use.

SUGGESTION: Always remember to re-condition your battery every holiday period. The battery re-conditioning process is as follows:

- Fully charge the MacBook's battery.
- Disconnect the power and use your MacBook on battery power until fully discharged.
- After the MacBook shuts down reattach the power cable back into the MacBook and fully recharge the battery again.
- Repeat this process three times for a total of three full battery charges and three full discharges.

SOFTWARE UPDATES

Students have full Administrator Rights to their MacBook and it is the student's exclusive responsibility to ensure that is properly looked after and charged ready for use every day.

LIBRARY LOANS

All technology loans are managed from the College Library. The Library staff are responsible for the handing out and collection of technology at the start and end of each academic school year.

REPAIRS AND REPLACEMENT

If the machine becomes damaged in some way or the machine is not functioning properly it must be returned to the IT Department immediately. If the problem is serious you will be asked to take your MacBook to the Library which will be signed into the care of the IT Dept.

In the event that your son or daughter's MacBook cannot be repaired within the stated turnaround timeframe, he or she will receive a loan MacBook for the duration of the repair (subject to availability).

The distribution of these loan MacBooks are handled by Library.

MANAGING YOUR FILES AND SAVING YOUR WORK

- All data needs to be backed up regularly in case the machine fails and need to be reimaged.
- All-important school work and data should be saved to your google drive.
- Students are advised to get an external hard drive and use Time Machine to back up their MacBook.

REGULAR BACKUPS

Regular backups: The student must agree to regularly backup their files either on the network drive or an external hard drive. The IT department do not have the resources to spend time retrieving lost data and many computer problems will be solved by reimaging the computer.

SAFE USE OF TECHNOLOGY

How parents and carers can reduce the risks: There are specific things that parents and carers can do to reduce the risks associated with online activities. By taking responsibility for their son or daughter's online computer use, parents can greatly minimise any potential risks of being online. The following are suggested guidelines for parents and carers:

1. Be aware that excessive, unmonitored use of computers can be harmful. Excessive use has been linked to increased risk of obesity, repetitive-strain injuries, impaired vision, declines in social interaction, and feelings of loneliness and depression. It is recommended that parents limit the time children spend using computers and monitor the content of the sites their children visit or computer games they play.
2. Set reasonable rules and guidelines for computer use by your child. Discuss these rules with him or her and then post them near the computer as a reminder. Decide upon the time of day that students may be online, and the appropriate areas students can access. Monitor his or her compliance with these rules, especially when it comes to the amount of time your child spends on the internet, especially late at night, as this may be an indicator of potential problems.
3. Keep internet-connected computers in a communal area of your home with the screen facing outward. One of the most important ways to protect your child is to ensure that any such computer or game machine is not located in his or her room. Ideally, it should be placed somewhere in the house which is commonly used by everyone, that is, where it is quite normal to pass through and notice what is happening.
4. Be clear about what you consider to be unacceptable online information or communication.
5. Become an internet user yourself and get to know any services your son or daughter uses. You will then have a better understanding of the way the technology works and it will not seem unusual that you are interested in his or her online activities.
6. Instruct your child not to respond to messages that are suggestive, obscene, belligerent, threatening, or make him or her feel uncomfortable. If they receive such a message, forward a copy of the message to your Internet Service Provider (ISP), and ask for their assistance.
7. Encourage your son or daughter not to access any links which are contained in emails from persons they do not know. Such links could lead to inappropriate web sites.
8. Explain to your son or daughter that passwords, addresses, pin numbers, credit card details, phone and email details are all private and should never be given to anyone via the internet, particularly if that person is only known online.
9. If your child has his or her own email address, it is advisable that they do not give any indication of his or her age or gender.
10. Get to know your son or daughter's 'online friends' just as you get to know all his or her other friends.
11. Contact your ISP if your son or daughter encounters any inappropriate content or is subjected to any unsolicited contact by strangers online. Ask your ISP to find out what child-safety measures they offer. In addition, there are filtering features built into the popular internet browsers that empower parents to limit their child's access only to those sites that have been rated appropriate for children.

Regardless of what filtering software is used, the best way to assure that your child has positive online experiences is to stay in touch with what they are doing.

SOCIAL MEDIA

Social media (Facebook, Google+, and Twitter) has become one of the fastest-growing segments of the internet. In part, this is because many young people enjoy the interactive "playground" in which they can "chat" simultaneously to a group of other users, or to just one individual.

Increasing concerns are being expressed over children's excessive and unsupervised use of social media. There are obvious issues associated with young people sitting for hours in front of computer screens, such as

avoiding physical activity and contact with their families, as well as failing to spend time on necessary homework and study.

The second issue relates to safety. Students tend to use social media to connect with many individuals without understanding the limitations of what personal information they should or shouldn't be giving away. There are many resources provided by the College through educational programs and by the government via online resources.

SAFETY TIPS FOR STUDENTS

The following safety tips for students should be adhered to at all times:

- Be careful: People online may not be who they say they are.
- Protect your personal information. Never give out your email, home address, phone numbers or the name of your school.
- Never send a person your photograph or anything else without first checking with your parents.
- Never meet anyone you have met online unless you are sure who they are and have your parent's permission.
- Tell your friends or an adult if you find something online that makes you feel uncomfortable.
- Never download files from strangers or people you may not know well or trust.

PROXY SITES

The use of 'Proxy Sites' to access otherwise blocked websites is prohibited by College policy. If these sites are accessed outside the school environment, care should be taken not to transmit sensitive information (eg: usernames and passwords, bank details, etc…). Proxy sites may steal such information from using key-logging technology.

The websites below offer practical advice on internet safety, parental control and filters for the protection of children, students and families.

IDENTITY THEFT

Identity theft and fraud can occur through a process of 'phishing'. Through email or fake websites, someone could impersonate a legitimate organisation (such as a bank) to obtain personal information. This information can then be used to defraud. It is imperative that personal information is not revealed via email.

AUSTRALIAN ONLINE SAFETY LINKS

- Office of the Children's eSafety Commissioner

  https://www.esafety.gov.au/
- Stay Smart Online
  www.staysmartonline.gov.au/kids_safe_online
- Netalert: a toll free helpline and website for parents wanting to ensure safe Internet usage by their children. Netalert is a Federal Government project.
  www.netalert.net.au
- Australian Families Guide to the Internet: from the Australian Broadcasting Authority
  www.aba.gov.au/family/index.html

INTERNET AND PRIVACY

Glasshouse Christian College employs a content filtering program, Sophos, and also has sophisticated tools to enhance filtering including the ability to trace all sites visited by users, the time visited and even the search items used in a Google search.

A growing concern is the invasion of privacy that occurs when you choose to respond to online surveys, sign up for free services or when you purchase online. 'Spyware' programs are computer programs that are installed without the user's' knowledge and which gather information about someone without their knowledge, and 'Ad-ware' are programs which force their Adverts upon you. These sorts of programs are often unintentionally installed when users install games and software from unverified sources.

HOW WE USE COOKIES

A cookie is a small file which is placed on your computer's hard drive with your permission. If you grant permission, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

CYBERBULLYING

Cyberbullying is an increasing concern and can best be described as electronic bullying. It occurs when threats are made via email or mobile phone or when defamation occurs on the internet.

Cyberbullying has been defined as "when the internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person",[2] or as "when an electronic device is used to attack or defame the character of a real person. Often embarrassing or false information about the victim is posted in an online forum where the victim and those who know the victim can see it publicly.

Cyberbullying can be as simple as continuing to send email to someone who has said they want no further contact with the sender, but it may also include threats, sexual remarks, pejorative labels and terms, ganging up on victims by making them the subject of ridicule in forums, and posting false statements as fact aimed at humiliation.

Cyberbullies may disclose victims' personal data (e.g. real name, address, or workplace/schools) at websites or forums or may pose as the identity of a victim for the purpose of publishing material in their name that defames or ridicules them. Some cyberbullies may also send threatening and harassing emails and instant messages to the victims, while others post rumours or gossip and instigate others to dislike and gang up on the target.

Cyberbullying in any form is completely unacceptable at the College. Any student that has been found to engage in such behaviour may have their computer privileges revoked.

MONITORING AT COLLEGE

Students may encounter random audits on their MacBook by their teachers or the IT Department Staff. These checks include searches for inappropriate images, illegal downloads or non-standard software.

MONITORING AT HOME

It is important that parents understand that the internet filter employed at the College does not extend to the home and that parents need to provide for their child's online safety in the home.

MACBOOK INSPECTION

Students may be selected at random to provide their MacBook for inspection.

Students should be aware that the IT Department has visibility of the applications and software installed on students' MacBooks.

SAFE USE OF TECHNOLOGY - PHYSICAL ASPECTS

Guidelines for the Use of MacBook Computers

STRESS RELIEF

1. Organise your time to allow for frequent breaks. Students should have a five minute break from the use of a MacBook at least every thirty minutes.
2. Use the breaks to change what activity you're doing, or to move around flexing and stretching your muscles.
3. Use your MacBook on a firm surface, where it is at the correct height for keying.
4. Make sure you can sit comfortably with your arms and wrists horizontal. Your back should be upright and supported. Both feet should be flat on the floor.
5. Sit facing the keyboard squarely, and then adjust the angle of the screen to minimise reflections and glare. The correct angle should also mean that you avoid the need to bend your neck excessively.
6. Try to avoid glare from windows that reflect on the screen.
7. Learn to be more aware of your body so that you can recognise any unnecessary muscle tension, and then be able to release it.
8. Check your posture at regular intervals.
9. Always lift any heavy loads with a straight back. Use your thigh muscles when lifting.
10. You should not carry MacBooks while they are receiving transmissions from wireless networks.

TRAVELLING WITH A MACBOOK

Plan to carry the minimum load necessary between College and home. To lighten your total load, store books that you will not need overnight in your lockers/classrooms.

Remember to shift the weight from one side to the other, rather than favouring one side for long times when carrying loads. When you are waiting for transport, put your bag down and stretch your back.

PART II - POLICY AND PROCEDURE

ACCEPTABLE USAGE FOR STUDENTS

ONLINE COMMUNICATION

The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes.

Today's students are exposed to online communication tools and the internet in their community. Use of the internet and online communication services provided by the College is intended for research and learning and communication between students and staff.

Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their parents/carers/teachers.

Students who use the internet and online communication services provided by the College must abide by the College's conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

Students should be aware that a breach of this policy may result in disciplinary action in line with the College's discipline policy.

ACCESS AND SECURITY

- Students may not access the internet in any way except for through the College network which has the appropriate filters in place
- Students should not disable settings for virus protection, spam and filtering that have been applied as a school standard.
- Students should ensure that communication through internet and online communication services is related to learning.
- Students should keep passwords confidential, and change them when prompted, or when known by another user.
- Students should use passwords that are not obvious or easily guessed.
- Students should never allow others to use their personal e-learning account.
- Students should never attempt to hack someone's personal data.
- Students should promptly tell their supervising 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.
- Students should seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- Students should never knowingly initiate or forward emails or other messages containing:
    - a message that was sent to them in confidence.
    - a computer virus or attachment that is capable of damaging recipients' computers, chain letters and hoax emails.

- spam, e.g. unsolicited advertising material.

NEVER SEND OR PUBLISH:

- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments, threatening, bullying or harassing comments to another person or make excessive or unreasonable demands upon another person.
- Sexually explicit or sexually suggestive material or correspondence, false or defamatory information about a person or organisation.

Ensure that personal use is kept to a minimum and internet and online communication services are generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software or music/movies is not permitted.

Ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Be aware that all use of internet and online communication services can be audited and traced to the accounts of specific users.

PRIVACY AND CONFIDENTIALITY

Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests

INTELLECTUAL PROPERTY AND COPYRIGHT

Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the internet or intranet has the approval of the Principal or their delegate and has appropriate copyright clearance.

MISUSE AND BREACHES OF ACCEPTABLE USAGE

Students will be aware that:

- they are held responsible for their actions while using internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.
- the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

MONITORING, EVALUATION AND REPORTING REQUIREMENTS

Students will report:

- any internet site accessed that is considered inappropriate.
- any suspected technical security breach involving users from outside the College.

MONITORING OF COMMUNICATIONS

Students understand: that authorised staff at the College are able to track and view communications including content of email messages, chat sessions and other forms of electronic communications as required.