Lynwood Senior High School

Parent Funded MacBook Policy

Information for Parents and Students
Dear Parents / Guardian

Please find attached the Lynwood Senior High School Parent Funded MacBook Usage Policy, relating to the acceptable use of the Parent Funded MacBook computer at school and at home. **If you have any queries and/or require further assistance regarding these documents please do not hesitate to contact the school on 9354 0600**

Thanking you for your support in this matter.

Yours sincerely

Gary Anderson
Principal
Lynwood Senior High School

**Table of Contents**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Responsibilities</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3.1 The Role of Students</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3.2 The Role of Parents or Guardians</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3.3 The Role of Teaching Staff</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>3.4 The Role of the school</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Guidelines for proper care of MacBook</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5.1 Security and Storage</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5.2 Transport and Handling</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5.3 Occupational Health and Safety Guidelines</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Data Management</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Printing</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>Virus Protection</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>Digital Citizenship Agreement</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>7.1 Access Security</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7.2 Internet Usage</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>7.3 Cybersafety</td>
<td>6</td>
</tr>
</tbody>
</table>
INTRODUCTION

A MacBook Program is a parent funded program in which participating students own and use their own MacBook computer for use at school and home, enabling a more student-centred, experience-rich education relevant to the 21st Century. Students develop skills, work habits, attitudes and expertise that will prepare them for success and help them to become efficient and effective life-long learners.

The Department of Education supports students in the appropriate and safe use of their MacBook. By alerting parents and students to potential dangers, developing guidelines and providing advice and support, the exposure of students to potential problems can be minimised.

This document is specifically aimed at parents and students who are involved in the Lynwood Senior High School Parent Funded MacBook Program and details the policy, guidelines and support strategies to ensure that students are able to make effective use of their MacBook and avoid any problems.

Please note whilst the MacBook is a great learning tool, other resources and normal teaching practice is not being replaced.

RESPONSIBILITIES

2.1 The Role of Students

Students must use their MacBook computers and the school computer network responsibly. Communications on the information networks are often public and general school rules for student behaviour, conduct and standards will apply.

When using their MacBook and accessing school information resources students must follow the policy and guidelines detailed in this document.

Any student who fails to honour this Code of Conduct may forfeit use of their MacBook at school and access to the school network.

2.2 The Role of Parents or Guardians

Parents or guardians are required to take responsibility for conveying the importance of the policy guidelines in this document and other school policies to their children. They are also required to monitor their child’s use of the MacBook, especially at home, including access to media and information sources.

2.3 The Role of Teaching Staff

School teaching staff will monitor appropriate care of the MacBooks and use of the MacBooks in accessing curriculum information. They will also provide guidance and instruction to students in the appropriate use of such resources.

This includes staff facilitating student access to information on their MacBooks in support of and to enrich the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of students.
2.4 The Role of the School

The school commits to upholding and providing physical and financial resources to enable safe, educationally relevant access to the MacBooks and relevant curriculum facilities for staff and students.

The school also has a responsibility to ratify information published on the internet by students, or the school, under the school’s name meets legal requirements and community standards in relation to copyright and safety.

3 GUIDELINES FOR PROPER CARE OF MACBOOK

3.1 Security and Storage

When the MacBook is being used away from school, students should avoid leaving it unattended or where it is visible to the public (e.g. in a vehicle). In these circumstances, the MacBooks can become a target for theft.

When the MacBook is at home please ensure that normal accepted domestic security practices are followed. This would include locking the windows and doors in the home when the unattended.

3.2 Transport and Handling Procedures

Students will be required to purchase or use a protective cover in order to transport their MacBook. When transporting the MacBook, students are to make sure that it is in the cover and in their school bag which must be securely closed.

3.3 Occupational Health and Safety Guidelines

The basic health and safety guidelines for desktop computers also apply to MacBook use:

- Keep the upper arms relaxed at the side of the body
- Bend the elbows to around 90 degrees
- Keep the wrists straight

4 DATA MANAGEMENT

Saving or back-up of data is the student’s responsibility. To backup their work it is recommend that students purchase a USB flash drive or preferably, an external hard drive. If a MacBook needs to be reimaged, it will erase all data. Staff will not accept data loss as an excuse for not handing in work on time.

5 PRINTING

Technical staff will provide access to network printers. Printing will be supervised by the teacher and charged in the usual manner. Students must arrange for this to be conducted during class time or at another time convenient for the classroom teacher.

Students should minimise printing at all times by print-previewing, editing and spell-checking on screen, rather than on printouts before printing. Students should not load paper into printers without permission.

6 VIRUS PROTECTION

The Macbook image is not configured with anti-virus software.
DIGITAL CITIZENSHIP AGREEMENT

This policy is a written agreement that formally sets out the rules of use of information technologies. All staff and students accessing the Department of Education System are bound by Department of Education rules of use.

Digital Etiquette
The following is a list of the expectations students are to understand and accept when using their own devices or any school owned technological device.
1. Follow all teacher directions including when to use the device.
2. Have the volume of devices muted at the beginning of each lesson.
3. Use appropriate manners when communicating electronically.
4. Provide their device to teachers upon request.
5. Provide their device to parents upon request.

Digital Access & Use
Students are expected to access the various technologies offered by Lynwood SHS in an appropriate and safe manner. Students are required to maintain and clean their device. For BYO devices, students are required to bring them to school fully charged. Any incident of vandalism or damage to any electronic device needs to be reported as soon as possible.

Students are not permitted to:

- Bring or download unauthorised programs, including games, to the school or run them on school computers or BYO devices. Recreational internet games are banned on school premises.
- Create or connect to an unauthorised network during school hours (eg, adhoc and personal hotspots).
- Engage in any form of cyber bullying.
- Access social networking sites (such as FaceBook and Instagram) or video streaming sites (such as YouTube) whilst at school, unless under the direction of your classroom teacher.
- Use the camera or audio recording functions without permission from the teacher and are reminded that they must not publish photographs or recordings taken at school or at school events.
- Delete, add or alter any network configuration files.
- Distribute copyright materials including software, music and movies. Copyright is to be observed at all times.
- Deliberately introduce, use or possess any virus or program that reduces system security or effectiveness.
- Log into the network with any user name or password that is not their own, change any other person’s password, or attempt to alter any person’s access rights.
- Enter any other person’s file directory or do anything whatsoever to any other person’s files.
- Reveal their network password to anyone except to staff. Students are responsible for all activity on their accounts.
- Store the following types of files on the school network, without permission from their teacher:
  - Program files
  - Compressed files
  - Picture files, unless they are required by a subject
  - Inappropriate materials or filenames including obscene or offensive material
  - Password-protected file

The consequence of non-adherence to this policy will be dealt with under the School’s Managing Student Behaviour and Good Standing Policies.
7.1 Access Security

Monitoring and Logging
A log of all access to the internet including e-mail will be maintained and periodically scanned to ensure that undesirable internet sites have not been accessed and that the content of remains within the guidelines described in this document.

7.2 Internet usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way.

Because the Internet is a public environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene school rules or rules imposed by parents/guardians.

The school is aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

It is the responsibility of the school to:

- provide training on the use of the Internet and make that training available to everyone authorised to use the school’s internet link
- take action to block the further display of offensive or inappropriate material that has appeared on the internet links.

Students must not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or discussion intended to provoke a sexual response
- Violence, bullying and anti social behaviour
- Information about committing any crime
- Information about making or using weapons, booby traps, dangerous practical jokes or "revenge" activities

7.3 Cybersafety

Parents will be aware of many incidents reported in the media regarding online safety. Personal information is easily tracked and harvested by those who know how, so it is important to keep as safe as possible while online.

Parents are encouraged to check the following sites online for further useful information: