



# St Margaret's School Laptop Handbook 2017

# Student Laptop User Handbook

Issued: October 2016

Version: 1.0

## USING YOUR LAPTOP

### SAFE USE AND HANDLING OF YOUR LAPTOP

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

- You **MUST** backup your important documents, photos and data to external drives such as USB or cloud storage.
- The laptop comes bundled with a protective carry case. Students are required to store the laptop in this carry case at all times when moving the laptop from one location to another.
- **Before storing the laptop in the protective carry case, care should be taken to ensure that it has fully powered off to avoid overheating in the case, and any USB sticks, earphones etc. are removed to avoid breaking them.**
- Do not drop your laptop onto any hard surface (such as a desktop in the classroom). Damage can occur from even the slightest drop.
- 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 LCD.**

- The case and lid may be cleaned using a clean dampened cloth that has had any excess water squeezed out.
- Do not place heavy objects on your laptop screen.
- Dropping your bag with the laptop inside may cause severe damage to the computer.
- Do not allow drinks or liquids near your laptop. While the carry bag may protect your laptop from minor splashes, the bag is not water-proof. Therefore extra precaution should be taken even if your laptop is in the carry case.
- Do not force your laptop into tightly packed suitcases, bags or backpacks. The compression may cause damage to the laptop or crack the LCD screen.
- Students must use the reinforced carry bag issued for transport of the laptop to, from and around school.
- Do not attempt to disassemble or alter any part of the laptop. All repairs must only be performed by technicians authorised by IT Services.
- All damages must be reported immediately to IT Services.
- Do not scratch, dent or bend any part of the laptop.
- **The marking of your laptop/case/battery with stickers, pens, pencils or highlighters will be considered intentional damage. If the equipment has graffiti of any type anywhere, you will be expected to pay for the required repairs or replacement.**
- Do not place any objects between the keyboard and LCD screen.
- Do not pick up or hold your laptop by the LCD screen.
- Do not store your laptop where the temperatures are below 5°C or above 35°C (41°F and 95°F).
- Do not leave the laptop unattended at any time. All laptops must be kept secured either with you or locked in your locker.
- Only use the AC adaptor supplied with the laptop. Do not attempt to use a different brand or model for charging your laptop. Doing so may result in damage.
- It is essential that you fully charge your laptop each night at home so it is ready for school the next day.

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

- Charge the laptop's battery
- Disconnect the power and use your laptop on battery power until fully discharged.
- With the laptop turned off, plug the power cable back into the laptop and fully charge the battery again.
- Repeat this process another 2 times for a total of 3 full battery charges and 3 full discharges.

### SAFE USE OF TECHNOLOGY - GOING ONLINE

How Parents Can Reduce the Risks.

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

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, decline 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 daughter. Discuss these rules with her and then post them near the computer as a reminder. Decide upon the time of day that she can be online and the appropriate areas she can access. Monitor her compliance with these rules, especially when it comes to the amount of time she spends on the Internet, particularly 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 games machine is not located in 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. Consider creating an acceptable use contract that you and your daughter agree on with stated penalties for misuse.
5. Become an Internet user yourself and get to know any services your 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 her online activities.
6. Instruct your child not to respond to messages that are suggestive, obscene, belligerent, threatening or make her feel uncomfortable. If she receives such a message, forward a copy of the message to your Internet Service Provider (ISP) and ask for their assistance.
7. Encourage your daughter not to access any links that are contained in emails from persons she does not know. Such links could lead to inappropriate web sites, viruses and trojans.
8. Explain to your 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 daughter has her own email address, it is advisable that she does not give any indication of her age or gender.
10. Get to know your daughter's 'online friends' just as you get to know all her other friends.
11. Contact your ISP if your 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 she is doing.

#### Social Media

Social media (Facebook, Google+, 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 school 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.
- Hang on to 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.
- The use of 'Proxy Sites' to access otherwise blocked websites is prohibited by school policy. If these sites are accessed outside the school environment, care should be taken not to transmit sensitive information (e.g. usernames and passwords, bank details, etc...). Proxy sites may steal such information using key-logging technology.

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

#### Australian links

- Stay Smart On Line - <https://www.communications.gov.au/what-we-do/internet/stay-smart-online/youth>
- The Child Safety Network of Australia has a web site which aims to provide families, kids, teachers and other professionals with information about the safety of children. <http://www.childsafe.org.au/>

### SAFE USE OF TECHNOLOGY - PHYSICAL ASPECTS

#### Guidelines for the Use of Laptop Computers

1. Organise your time to allow for frequent breaks. Students should have a 5 minute break from the use of a laptop at least every 30 minutes.
2. Use the breaks to change what activity you're doing, or to move around flexing and stretching your muscles.
3. Use your laptop 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 laptops while they are receiving transmissions from wireless networks.



### Travelling With a Laptop

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

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.

If you are using a backpack, you must place both straps over the shoulders. You could even try carrying the load on the front of your body, to see if this is more comfortable.

### Use of Protective Carry Case

All students will be supplied with a protective carry case for use with the laptop. Protective carry cases are designed to minimise damage to the laptop during transportation and **students are required to use the carry case at all times including moving the laptop between classes.**

## LOAN LAPTOP POLICY

### Laptop Loan Pool

The student laptop loan pool consists of laptops with comparable specification and functionality to the laptops the students use.

### Purpose of a Loan Laptop

As the laptop supplied is to be used as a tool for accessing educational resources, IT Services technical staff will endeavor to have any non-working laptop repaired and returned to the student within 48 hours. In the event that your daughter's laptop cannot be repaired within the stated turnaround timeframe, she will receive a loan laptop for the duration of the repair (if one is available). A pool of laptops is available for this purpose, with the maintenance and distribution of these loan laptops being handled by IT Services Department.

### Student Data Availability During Repair Period

Students who are issued with a loan laptop will have all their data transferred from their own laptop to the loan laptop if possible. In certain circumstances recovery of data from the hard disk may not be possible and a restore from the student's own backup will be required.

### Use of Laptops by Students on Loan Basis

As noted above, IT Services maintain a pool of laptops which are available for students to use on a loan basis. The following is a list outlining the correct use and care of the loan laptop:

1. A Loan Authority Form (stating the terms and conditions for laptop loans) must be filled out and signed by the student before the loan laptop can be released.
2. Students must not apply any stickers or markings to the loan laptop.
3. Students must not leave loan laptops unattended at any time.
4. Loan laptops are not to be given to anyone other than the signed borrower.
5. No alterations or attempted repairs are to be performed on the loan laptop. All laptop repairs are performed by technicians authorised by IT Services.



### **Loan Periods**

While there is no fixed time period for the loaning of laptops (based on the nature of repair required by the original laptop), students must return the loan unit within 24 hours of being notified that their laptop has been repaired. This is to ensure that loan laptops are available for other students who may need them.

### **Laptop Accessories**

All laptop accessories provided with the loan laptop, such as AC chargers or bags, must be returned at the completion of the loan period. Items not returned will be billed to the parent account for payment.

## APPENDIX

### Online Communication Services: Acceptable Usage for Students

#### 1. Objectives - Policy statement

1.1 The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links provide students with a collaborative learning environment and are intended to assist with learning outcomes. Students today are exposed to online communication tools and the internet within their community.

1.2 Use of the internet and online communication services provided by the school, is intended for research 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.

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

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

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

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

#### 2. Audience and applicability

2.1 This policy applies to all school students who access internet and online communication services within the St Margaret's School network and from any external location.

#### 3. Responsibilities and delegations

##### 3.1 Access and Security

Students will:

- not bring 3G/NextG or other network connectivity devices to use at school which bypass the internal control systems
- not disable settings for virus protection, spam and filtering that have been applied as a school standard
- ensure that communication through internet and online communication 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
- never allow others to use their personal e-learning account
- log off at the end of each session to ensure that nobody else can use their e-learning account
- 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
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student
- 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, graphics or music that is not associated with learning is not permitted.
- never damage or disable computers, computer systems or networks of the school
- 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.

### 3.2 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.

### 3.3 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.

### 3.4 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.

## 4. Monitoring, evaluation and reporting requirements

### 4.1 Students will report:

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

### 4.2 Monitoring of communications

Students understand:

- that authorised staff of the school are able to track and view communications including content of email messages, chat sessions and other forms of electronic communications as required.