Meridan State College
1 to 1 Take Home Laptop Charter

Student Charter

MERIDAN

Contents

Student 1to1 Charter

1to1 overview

The Meridan State College 1to1 program, has been born out of the completion of the NSSCF program. As a college, we have decided to provide 2 programs at the college for students to participate in to enable a true 1to1 learning experience.

The 2 programs that Meridan State College has created are the BYOx program, where students provide their own device, which is then connected to the college's WiFi network, enabling their own tailored technology experience and the 1to1 Program, where the students hire a college provided device , Productivity software, and free access to college purchased software e.g. Adobe Creative Cloud.

These programs will allow students to have a true 1to1 experience, allowing them to take work with them, install additional software to enhance or assist in their learning, the ability to make electronic notes and carry digital textbooks provided by the Resource Centre.

All devices used in the program are the property of Meridan State College.

This program only supports college owned ICT assets being provided to students for educational use at school or at home.

Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines.

Data security and back ups

Students must understand the importance of **backing up data** securely. Should a hardware or software fault occur, assignments and work that has taken a considerable time to prepare may be lost.

The student is responsible for the backup of all data. The backup of the data on the device is the responsibility of the student and should be backed-up on an external device, such as external hard drive or USB drive. **The school will take no responsibility for lost data, resulting in lapsed assessment timelines, and extensions are not normally given for such circumstances.**

Students should also be aware that, in the event that any repairs need to be carried out the contents of the device may be deleted and the storage media reformatted.

Acceptable computer and internet use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within

the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems.

This policy also forms part of this Student 1to1 Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the college grounds.

Communication through internet and online communication services must comply with the Responsible Behaviour Plan available on the college website.

In adhering to the acceptable use of ICT and Responsible Behaviour Plan, Students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the college standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems or Queensland DOE networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

Passwords must not be obvious or easily guessed; they must be kept confidential, and changed when prompted or when known by another user.

Personal accounts cannot be shared. Students should not allow others to use their personal account for any reason.

Students should log off at the end of each session to ensure no one else can use their account or device.

Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online today are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation.

Cybersafety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent and/or caregiver as soon as is possible.
Students are encouraged to explore and use the "Cybersafety Help" button to talk, report and learn about a range of cybersafety issues.

Students must seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students must never initiate or knowingly forward emails, or other online content, containing:

- A message sent to them in confidence
- A computer virus or attachment that is capable of damaging the recipients' computer
- Chain letters or hoax emails
- Spam (such as unsolicited advertising).

Students must never send, post or publish:

- Inappropriate or unlawful content which is offensive, abusive or discriminatory
- Threats, bullying or harassment of another person
- Sexually explicit or sexually suggestive content or correspondence
- False or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to visit the Department's Cybersafety Web Page

Web filtering

The Department of Education (DOE) operates a web filtering system to protect students and restrict access from malicious web activity and inappropriate websites.

The DOE Web filtering system is installed on departmentally-owned computers, including Computer for Student (CFS devices). There is also a locally installed Web filtering client, which resides on the device and is active when using a non-DOE wireless connection to ensure filtering is always applied.

When students are connected through DOE managed networks they will have a high level of filtering applied. This level restricts them from websites such as:

- Social networking sites e.g. Facebook
- Open/Mixed content sites e.g. YouTube
- Translation sites e.g. Google translation
- Chat sites e.g. MSN Messenger
- Internet telephony e.g. Skype
- Media Sharing e.g. Prezi

When students use their devices at home the filtering system (proxy client), functions with two levels of filtering, **high** (more restrictive) and **medium** (less restrictive).

A **high** level of filtering at home provides a less restrictive access level then that at the college however a greater level of protection than medium. Websites and web applications that are blocked at the college but are available to students at home include:

- Blogs/personal pages
- Chat/Instant Message e.g. MSN Messenger
- Internet Telephony e.g. Skype
- Media Sharing e.g. Flickr
- Online Storage e.g. Dropbox
- Software downloads

In partnerships with schools, parents/caregivers can allow their child medium level filtering when they are connected to a non-departmental internet connection, such as their own home internet.

Medium level filtering provides a less restrictive level of protection. Students with this level can access a wider range of websites, which include:

- Social networking e.g. Facebook
- Adult/mature content
- Alternative spirituality/belief
- Nudity
- Translation websites

It is important to remember filtering systems do not replace the need for parental supervision when students are online.

If parents/caregivers allow their children to have a medium level of filtering at home, they need to be aware that the child's online activities are the shared responsibility of the parent and the student. This process requires sign off of the Student Charter Agreement indicating your willingness to support your child's access to medium filtering.

Parents, caregivers and students are encouraged to visit the Cybersmart website at

www.cybersmart.gov.au.

For further information on the web filtering system visit the Smart Classrooms website:

http://education.qld.gov.au/smartclassrooms/enterprise-platform/web-filtering/index.html

Students' reporting requirements

Students are required to report any internet site accessed that is considered inappropriate.

Any suspected security breach involving students, users from other schools, or from outside the Queensland DOE must also be reported to the college.

Privacy and confidentiality

It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. It should also be ensured that privacy and confidentiality is always maintained.

Intellectual property and copyright

Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their 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.

Software

The software loaded on the device is licensed to the DOE or the college. The parent or caregiver must ensure that the software is not copied, deleted or transferred, without prior written consent from the school. Unauthorised use may breach copyright laws and the parent or caregiver may be held liable for any damages incurred.

Elevated access

Devices may have elevated permissions which would provide the ability to complete tasks such as installing home items including home printers, cameras and/or licensed software.

This access may allow further permissions above and beyond those available on other MOE (Managed Operating Environment) built workstations and devices. Students should not misuse these privileges. The misuse of this access may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

If given elevated access, students have the ability to install additional software onto the device. However, only licensed software can be installed. The student must hold a valid license for any software installed and the license must be appropriate for installation on the device. Devices may be audited by a school representative requiring students to present a valid software license for any personal software installed. Devices may be rebuilt at any time for numerous reasons without consultation with students or parents and all local data may be lost in this process.

The college will manage the provision of elevated access and may require a parent/ caregiver to approve, using the form at the back of this document.

Monitoring and reporting

Students should be aware that all use of Internet and online communication services can be audited and traced to the account of the user.

All material on the device is subject to audit by authorised college staff. If at any stage there is a police request, DOE may be required to provide the authorities with access to the device and personal holdings associated with its use.

Loan equipment

The loan equipment referred to in this charter are a 11" to 12" Ultra Portable laptop and power pack; protective hard carry case and DOE's standard suite of software, which includes Microsoft Office.
Each device will be:

- protected by anti-virus tools and automated updates
- able to be connected to the school network and have filtered internet and email
- able to be used at home and at school for student learning
- installed with DOE's standard suite of productivity software
- Protected by Computrace theft protection.

Equipment ownership

At the end of the loan period, all devices will be returned to the college. The devices will have all licensed software and data removed and will be restored to their original factory state. Meridan State College will make a decision regarding the disposal, sale or recycling of the used devices, as appropriate at that time.

If the student completes their schooling or transfers from the college, the device must be returned to the college. If the device is not returned, reimbursement will be sought.

It is also a requirement of using the device that students provide authorised college staff with access to the device and personal holdings associated with the use of the device if requested.

Fee for provision of device

To participate in the college's 1to1 program, there is a cost involved for the provision and delivery of the device. This will cover costs incurred by the college in providing and supporting the device.

The items below are included in Meridan's standard 1to1 package:

Device item	Annual Cost Per Student
Device	Included
Protective Case	Included
Internet Filtering	Included
Windows 8.1 Operating System	Included
Microsoft Office Software Suite	Included
Antivirus Software	Included
Technical Support	Included
Hotswap (Where possible)	Included
School Based Software	Included
Laptop Tekskin	Included

Our college P&C has endorsed a co-contribution of $250 to be charged per device per annum (pro-rata charge available) for the device hire.

Damage or Loss of Equipment

All devices hired out through Meridan State College's 1to1 program are covered by a fair use policy. Instances where the hard disk fails or the LCD screen becomes faulty will be assessed and covered by the college to ensure your student has a fully operational device.

There is no cover for negligence, abuse or malicious damage. Students will be required to replace lost or damaged chargers or cases.

Any software or hardware issues, vandalism, damage, loss or theft of the device must be reported immediately to the college

Theft and loss

If the device is stolen outside of college, the parent/carer will need to report the incident to the police and ensure they have the following documentation when informing the college:

Police crime number; and

Statutory declaration (usually completed with the police).

Should a device be unrecoverable – whether lost or stolen, the full replacement cost of the device will be required

Non-Warrantable damage

Non-warrantable damage is where damage to the device would not be classified as a warranty claim. E.g. hard disk failure, LCD backlight failure, non-responsive keys on the keyboard are classified as warranty.

- Damage caused by not carying the laptop in the provided hard case.
- Any keys being removed from the notebooks keyboard due to excessive force applied.
- Leaving objects (such as pens) on the keyboard when closing the notebook lid, and as a result the LCD display is damaged.
- Leaving the notebook unattended and as a result the device is damaged.
- Willfully damaging the device by drawing or scratching the device with a sharp implement.

Faults are deemed as non-warrantable by the school, the below charges will apply

- Repair of the LCD screen is $100
- Replacement keyboards with damaged key cups is $40
- Damaged charger with broken or exposed wires is $35
- Damage from dropping device (upper or lower case), not including LCD screen is $100
- Graffiti to hard protective case is $35

NB: Where the college determines that damage has been intentionally caused to a device, the full cost or replacement of the device may be charged. This is a college managed process. Photographic evidence will be taken and kept on file for recording purposes; furthermore a replacement device may be refused or repaired device will not be issued/re-issued until payment is made.