SMART Classrooms

National Secondary School Computer Fund

Goomeri State School P-10

2015 Student NSSCF Charter

This document needs to be carefully read and signed by the student, parent/caregiver and a school representative before the NSSCF device is issued to a student.

Australian Government

Toward **Q**
Tomorrow's Queensland

Queensland Government

Contents

Australian Government

Toward **2** | Tomorrow's Queensland

Queensland Government

Student NSSCF Charter

NSSCF overview

The National Secondary School Computer Fund (NSSCF) is the major funding element of the Digital Education Revolution (DER). It is assisting with the provision of new computers and other information and communication technologies (ICT) equipment for students in Years 8 to 12. The aim of the NSSCF is to achieve a computer to student ratio of one-to-one for students in Years 8 to 12 by 31 December 2011.

The implementation of NSSCF is happening in partnership with the Australian government and the Queensland state government.

NSSCF is providing laptop computers (referred to throughout this document as the 'device') as a tool to assist student learning – both at school and at home. Students and parents/caregivers are asked to lend their support to this very valuable and innovative program. Strong support from parents and caregivers is paramount to ensure the program is successful and that students gain the maximum benefit.

The device that has been bulk purchased by the Department of Education and Training (DET) for the third NSSCF round (Q3) to Queensland state high schools is the Acer Aspire 1830T. This device was chosen based on a number of criteria, including portability, battery life, hardware capabilities, overall cost, warranty and support models.

All computers used in the program are the property of the Queensland DET.

This program only supports school owned ICT assets funded under the NSSCF, being provided to students for educational use at school and at home. In order to maintain the security of DET's network and support Managed Operating Environment (MOE), privately-owned devices cannot be connected to the network.

Loan equipment

The equipment referred to in this charter are the devices that were bulk purchased for Q3 and consists of a laptop computer and power pack; crush-proof carry case; 3G connectivity; and DET's standard suite of software, including Microsoft Office.

Each device will be:

- protected by anti-virus tools and automated updates
- covered by a four year warranty, including the battery
- covered by accidental damage protection (excess applies)
- able to be connected to the school network and have filtered internet and email
- provided with 3G connectivity
- able to be used at home and at school for student learning
- installed with DET's standard suite of productivity software
- protected by Computrace theft protection.

Equipment ownership

At the end of the loan period, all devices are returned to the school and will be removed from the school network. The devices will have all licensed software and data removed and will be restored to their original factory state. DET 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 school, the device must be returned to the school. If the device is not returned, reimbursement will be sought.

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

Fee for provision of laptop

To participate in the laptop home-use program parents and/or caregivers may be required to make a contribution. This will cover additional costs incurred by the school in providing and supporting the laptop.

Funding has been made available by the Federal and State Government for the implementation of the program; however schools may choose to provide extra management and support in addition the standard NSSCF package.

Australian Government

Toward 2 Tomorrow's Queensland | Queensland Government

The items below are included in Queensland's standard NSSCF package:

Device item	Annual cost per student
Laptop	Included
Vendor-operated student help desk	Included
Crush-proof protective case	Included
Accident damage protection	Included
Theft protection software	Included
Internet filtering	Included
Windows 7 operating system	Included
Microsoft Office software suite	Included
Antivirus software	Included
3G connectivity	Included

The following items and services are included in the **Goomeri State School P-10** take-home package for students:

Device item	Annual cost per student
Maintenance & On-Site Support	$90.00

Our school P&C has endorsed a co-contribution of $90.00 to be charged per device, per annum.

Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Detailed advice for the care of the device can be found in the Parent and Student Guide.

Data security and back ups

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

The student is responsible for the backup of all data. While at school, students are able to save data to the school's network which is safeguarded by a scheduled backup solution.

They are also able to save data locally to the device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as external hard drive or USB stick.

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 ICT-PR-004 Using the Department's Corporate ICT Network.

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

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

There are a few conditions that students should adhere to. 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 school standard

- use unauthorised programs and intentionally download unauthorised software, graphics or music

- intentionally damage or disable computers, computer systems or Queensland DET 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 laptop.

Cybersafety

At any time, if a student believes they have received a computer virus or spam (unsolicited email), or they have received a message 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 messages, 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 or publish:

- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments

- Threats, bullying or harassment of another person

- Sexually explicit or sexually suggestive material or correspondence

- False or defamatory information about a person or organisation.

Web filtering

An internet filtering solution provides DET with the ability to restrict access to inappropriate material on DET's ICT network.

Content filtering is active 100% of the time on the Computer for Student (CFS) devices. The filtering system is installed on each device, and will work regardless of whether the device is connected to a school, home or other network.

To help keep students safe when using the DET network (including the 3G connection), DET imposes a 'high' level of internet access filtering. A 'high' level provides a greater level of protection and therefore a high level of restriction. Sites that are blocked under a high level of internet access include:

- Social networking sites such as Facebook

- Open/Mixed Content such as YouTube

- Language translation sites

- Internet telephony sites such as Skype

- Alternative sexuality/lifestyles

- Intimate apparel/swimsuit.

Parents, in partnership with the school, may choose to allow students a 'medium' version of web filtering when working on a non-departmental network, such as a home wireless. The medium level filter provides a more relaxed level of protection for students. Students are able to access all of the types of sites listed above.

It is important to remember filtering systems are not foolproof and do not replace the need for parental supervision when students are online. Parents, caregivers and students are encouraged to visit the Cybersmart website at www.cybersmart.gov.au.

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 maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

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.

Damage or loss of equipment

All devices and batteries are covered by a manufacturer's warranty which covers manufacturing defects through normal usage. In addition, devices are covered by an insurance policy which protects against accidental damage. There is no cover for negligence, abuse or malicious damage. Students will be required to replace lost or damaged chargers.

Costs incurred by the school for the repair or replacement of devices may be charged by the school as an excess to parents. In the event of non-compliance of agreed responsibilities, schools may review the student's continued participation in the take-home program.

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

Theft and loss

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

- Police crime number; and
- Statutory declaration (usually completed with the police).

On receipt of the necessary documentation, DET will initiate recovery procedures via in the inbuilt theft protection software.

Should a device be unrecoverable – whether lost or stolen, the cost of replacement is as follows:

- First case: $200, payable by the parent/caregiver
- Subsequent cases: full replacement cost.

Accidental damage

Where a device is accidentally damaged, schools will invoice a student's parents according to the following sliding scale:

- First incident: $50
- Second incident: $100
- Subsequent: $150

Wilful and malicious damage

Where a school determines that damage has been intentionally caused to a device or a student has disrespected school property, the full cost of repair or replacement may be charged.

Software

The software loaded on the device is licensed to the DET or the school. 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.

Students may have the ability to install additional software onto the laptop. However, only licensed software can be installed. The student must hold a valid licence for any software installed and the licence must be appropriate for installation on the laptop. Devices may be audited by a school requiring students to present a valid software licence 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.

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-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.

The school 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 school staff. If at any stage there is a police request, DET may be required to provide the authorities with access to the device and personal holdings associated with its use.

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 DET must also be reported to the school.

Australian Government

Toward 2 Tomorrow's Queensland | **Queensland** Government

SMART
Classrooms

Student NSSCF Charter agreement

The Student NSSCF Charter agreement form must be signed and returned to the school before the device is issued.

The student and parent or caregiver must carefully read this charter before signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

In signing below, I acknowledge that I,

- accept all policies and guidelines as per the Responsible Behaviour Plan for Students

- understand my responsibilities regarding the use of the device and the internet

- acknowledge that I understand and agree with all of the conditions detailed in the Student NSSCF Charter

- agree to the provision of a (tick one)
    - □ **medium** (access to social media sites)
    - □ **high** (blocked social media sites, including YouTube)
  internet filtering with the assignment of the device

- understand that failure to comply with the Student NSSCF Charter could result in recall of the device and/or loss of access for home use

- agree to contribute **$90** for my child to access the take-home component of the National Secondary Schools Computer Fund program.

Australian Government

Toward 2
Tomorrow's Queensland

Queensland Government

After reviewing and understanding the responsibilities outlined in the *Acceptable computer and internet use* section above and relevant documents, I:

□ **agree** to the provision of elevated access associated with the assignment of the student device.

□ **do not agree** to the provision of elevated access associated with the assignment of the student device.

Student's name	**Signature of student**	**Date**

Parent / caregiver's name	**Signature of parent / caregiver**	**Date**

Designated school representative's name	**Signature of school representative**	**Date**

Australian Government

Toward 2 Tomorrow's Queensland | **Queensland** Government