National Secondary School Computer Fund

Student NSSCF charter

2015
Contents

Student NSSCF Charter ......................................................... 3
NSSCF overview ................................................................. 3
Device care .............................................................................. 4
Data security and back ups ....................................................... 4
Acceptable computer and internet use ....................................... 5
Passwords ................................................................................ 6
Digital citizenship ...................................................................... 6
Web filtering ............................................................................. 7
Students' reporting requirements ............................................... 9
Privacy and confidentiality ......................................................... 9
Intellectual property and copyright ............................................ 9
Misuse and breaches of acceptable usage ................................... 9
Software .................................................................................. 9
Elevated access ......................................................................... 10
Monitoring and reporting ......................................................... 10
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 9 to 12. The NSSCF achieved a computer to student ratio of 1:1 for students in Years 9 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 working in partnership with schools for the provision of devices as a tool to assist student learning. 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 are connected any time anywhere to their learning.

All devices used in the program are the property of the Queensland DETE.

This program only supports school-owned ICT assets funded under the NSSCF, 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.

Additional detailed advice for the care of the device can be found in the NSSCF Parent and Student Guide located on the Smart Classrooms website (http://education.qld.gov.au/smartclassrooms/enabling-learners/nsscf/index.html).

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. 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 drive.

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

This policy also forms part of this Student NSSCF 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.

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 school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems or Queensland DETE 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 and Cyberbullying document at http://education.qld.gov.au/studentservices/behaviour/qsaav/docs/cyberbullying-cybersafetyprintfriendlyguide.pdf

Web filtering

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

The DETE 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-DETE wireless connection to ensure filtering is always applied.

When students are connected through DETE 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

Students using DETE 3G connections to access the internet will still have a high level of web filtering applied.
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 than at school however a greater level of protection than medium. Websites and web applications that are blocked at school 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 DETE must also be reported to the school.

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 DETE 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.
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 licence for any software installed and the licence must be appropriate for installation on the device. 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.

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, DETE may be required to provide the authorities with access to the device and personal holdings associated with its use.
National Secondary School Computer Fund

Damage or loss of equipment

All laptops and batteries are covered by a manufacturer's warranty which expires at the end of Term 3, 2015. This covers manufacturing defects through normal usage. In addition, laptops 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 laptop must be reported immediately to the school.

Theft and loss

In the case of loss or suspected theft, a parent or guardian should lodge a report with the nearest police station. It is important that the following be recorded and provided to the school:

- the crime report number
- the name of the police officer who took the report.

In both cases, a witnessed statutory declaration should be provided to the school.

On receipt of the necessary documentation, the NSSCF program will initiate recovery procedures via Computrace theft protection software. Should a device be unrecoverable, the cost of replacement is as follows:

- First case: $200
- Subsequent cases: full replacement cost.

Accidental damage

Where a laptop 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.
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/caregiver must carefully read this charter before signing it. Any questions should be addressed to the school and clarification obtained before signing.

In signing below, we acknowledge that we,

- accept all policies/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 NSSCF program up till the end of Term 3, 2015.
- Should a student leave the school without returning the NSSCF device, attempts by school staff requesting the return of the device will be made. If attempts are unsuccessful, it will be deemed stolen property and escalated to Queensland Police

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

- [ ] 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.

I also understand that it is a requirement to participate in the Take Home Laptop/Tablet Scheme, I must have paid (or continue to pay, in the case of a payment agreement) my Student Resource Scheme Fee for 2015.

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 ______________