DEPARTMENT OF EDUCATION AND TRAINING

SMART Classrooms

National Secondary School Computer Fund

Q3 School Management Procedures Guide

Australian Government

Toward Q4 Tomorrow's Queensland

Queensland Government

Contents

National Secondary School Computer Fund overview

The National Secondary School Computer Fund (NSSCF) is the major funding element of the Australian Government's 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 aim of the NSSCF is to achieve a computer to student ratio of 1-to-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.

The Queensland Department of Education and Training (DET) is committed to achieving a 1-to-1 computer to student ratio in Years 9 to 12 by 31 December 2011.

Round three (Q3)

During round three, referred to as Q3, the Department of Education and Training ran a closed tender process to provide a bulk-purchased device.

The device chosen for 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 package.

A version of DET's Managed Operating Environment (MOE) has been installed on the NSSCF devices. This build version is unique to devices purchased under the Q3 bulk procurement.

Each of the bulk-purchased devices is 3G-enabled, providing students with 2GB of filtered internet downloads per month, for the life of the device.

Supporting materials

Student NSSCF Charter

NSSCF Parent and Student Guide

NSSCF Parent and Student Support Manual

School Technician Manual

OAMPS User Manual

All of these documents are available on the:

https://team.oneportal.deta.qld.gov.au/sites/NSSCF_Rollout/default.aspx

Acer Aspire 1830T technical specifications

The ultra-low voltage device provided under Round Q3 of the NSSCF is an Acer Aspire 1830.

The technical specifications are as follows:

· Intel Core i3 380UMB (1.33GHz) processor

· 4GB (2 x 2GB DDR3) memory

· 11.6-inch HD 1366 x 768 (WXGA) LED-backlit TFT LCD screen

· 320GB SATA II 7200RPM hard disk drive

· Intel Centrino® Wireless-N 6200 a/b/g/n

· 100/1000 Mbps integrated network interface

· Ericsson F5521GW 3G module

· Bluecoat internet filtering protection

· Bluetooth® 2.1+EDR

· Integrated VGA (640 x 480) webcam

· Full sized keyboard

· 6-cell Li-ion battery (63W 8500mAh)

· Four year warranty

· Accidental damage cover (excess applies)

· Targus crush-proof protective case

· Sim for 3G roaming connectivity (data plan inclusive)

· Protection and theft deterrence is provided by Computrace (excess applies).

Please note: if your school is running a take home program, it is predetermined that each device will be assigned to an individual student login, unless it is assigned as a pool device. This is managed through OAMPS.

Pre-loaded software

All devices come pre-loaded with the department's Managed Operating Environment (MOE), which includes a number of components.

The software pre-loaded on the device is licensed to DET.

Parents and caregivers must ensure the software is not copied, deleted or transferred, for any reason without the written consent of the school.

The table below shows what is pre-loaded onto each device:

	Application name	Vendor	Version
1	Office 2010 Professional Plus	Microsoft	14.0.4763.1000
2	Producer for PowerPoint	Microsoft	3.0.3012.0
3	Adobe Reader	Adobe	10.0.1
4	Adobe Shockwave	Adobe	11.5.9.620
5	Adobe Flash 10	Adobe	10.3.181.22
6	Adobe AIR	Adobe	2.6
7	Quicktime	Apple	7.6.9
8	Java	Oracle	6.0.26
9	PDF Creator	Adobe	1.2.1
10	SCCM Client	Microsoft	4.0
11	Office Clipart	Microsoft	10.0.2619.0
12	PhotoStory 3	Microsoft	3.0.1115.11
13	Audacity	Open Source	1.2.6
14	IrFanView	Open Source	4.28
15	Movie Maker	Microsoft	2.6.4038.0
16	Paint.net	Microsoft	3.5.8

	Application name	Vendor	Version
17	Silverlight	Microsoft	4.0.60310.0
18	Symantec End-Point Protection	Symantec	11.0.6300.803
19	Microsoft App-V Client	Microsoft	4.6.1.20870
20	.net Framework	Microsoft	4
21	Service Pack	Microsoft	1
22	Cyber Safety Button	Australian Federal Gov	n/a
23	Pointing Touchpad Application	Synaptics	14.0.6. 170909
24	e-Power Management System	Acer	n/a
25	Blue Coat	Blue Coat Systems	n/a
26	Computrace	Absolute Software	n/a

Loading additional software

Students may have the ability to install additional software onto the device (please see the Elevated access section below). 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 required to be rebuilt for numerous reasons. Students and parents need to be aware that any data saved locally or software installed from home may be lost in this process. Regular backups can reduce the possibility of important data or student work being lost.

Elevated access

Students may be allocated elevated permissions which would provide the ability to complete tasks such as installing home devices including printers, cameras and/or licensed software.

This access will 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 the Student NSSCF Charter.

Elevated access is allocated using the Operational Asset Management Provisioning System (OAMPS). See the ‘How to change a single student’s permissions’ section in the OAMPS Guide. This document can be found in the documents section of the Q3 Rollout Community.

SCCM software packages

Available on all National Secondary School Computer Fund devices, the **System Center Configuration Manager (SCCM)** is a Microsoft technology that provides schools with extended capabilities in the management and distribution of operation system and software patches.

It also allows for a managed environment to deploy packaged application software installations and allow integrated support for the next version of MOE 3.0.

SCCM replaces the Systems Management Server.

Benefits and required enhancements to support technologies, such as Windows 7 include:

- asset intelligence and awareness
- configuration management extensions
- enhanced software distribution
- software update management
- mobility support.

These new capabilities will ensure the security and integrity of the departmental network is aligned to industry standards.

For more information visit the SCCM team site. Frequently asked questions are also available on the site.

Network connectivity

NSSCF Q3 devices are able to connect to any wired or wireless network, allowing students to access the internet at school and at home. Complications may arise when trying to connect to the school network if settings for the wired network have changed.

Any device experiencing wired connectivity issue should be reset back to the default settings (instructions can be found in the School Technicians Manual, which is located on the Q3 Rollout Community)

Wireless

Wireless uses profiles to connect to the network. QDETA-X and IDET profiles are included in the NSSCF Q3 build and cannot be edited by students.

3G

Under the bulk supply of Q3 devices, each device will include a 3G data service to enable a greater level of mobility and flexibility for students to access online resources.

The 3G data service is a four year plan and provides 2 gigabytes (2GB) of data per month.

Home or private networks

Students with 1-to-1 devices are free to connect the device to any network. This, however, may cause some technical issues. Different networks require different configurations, and as such, are classed as unsupported.

Students are advised to contact the network administrator or internet service provider (ISP) for support of non-departmental network configurations.

Advice about connecting to a home network can be found in the NSSCF Parent and Student Support Manual.

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 Device 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 device.

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.

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.

Web filtering

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

Content filtering is active 100 per cent of the time on the Computer for Student (CFS) devices. The filtering system is installed on each departmentally-owned device, and will work regardless of whether the device is connected to a school, 3G or private network.

For more information about web filtering, visit the Smart Classrooms website.

Blocked web content

If a student tries to visit a website that is blocked under the web filtering system, they will be presented with either a departmental 'STOP' page or 'Internet Explorer cannot display the webpage' notification.

Examples where a site may be blocked include:

- the site is deemed to be inappropriate
- the site has not yet been approved as appropriate; or
- the site cannot be confirmed as permissible.

Web content filtering levels at school

High level filtering

To help keep students safe when using the DET network (including the 3G connection), the department imposes a 'high' level of internet access filtering. A '**high**' level of filtering provides a greater level of restriction and therefore greater level of protection. 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.

Choosing a different web content filtering level

Medium level filtering

In partnership with schools, parents/caregivers can allow their child '**medium**' level filtering when not connected to the DET network.

The medium level filter provides a more relaxed level of protection for students, where they are able to access all of the types of sites listed above.

The provisioning of '**medium**' or '**high**' levels of internet access is covered in the Student NSSCF Charter agreement, where, in consultation with the school, parents can request the access they wish their student to have.

Schools will manage the provisioning of high and medium levels of internet access on Q3 NSSCF devices, by using OAMPS.

Requesting web content approval

If a student or parent identifies a site they believe is incorrectly filtered (blocked or allowed), they should contact the school to request appropriate review.

For more information on content filtering visit the Smart Classrooms website below:

http://education.qld.gov.au/smartclassrooms/mis/filtering.html

Device security

Lost or stolen

DET uses a software asset tracking application called Computrace. This application aids in the recovery of lost and stolen devices. The software will be used only in the event of a reported theft or loss of a device.

Because all NSSCF devices belong to DET, it is important the loss or theft of a device is reported as soon as possible to the school and the Police.

Lost or stolen procedures

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).

Once the parent/caregiver has notified the school and produced the documents above, the school should look up the NSSCF device identification (ID) number in OAMPS and then log a job with the Service Centre 1800 680 445.

The Service Centre will notify the NSSCF team so a replacement device can be sent to the school.

If the device is stolen from within the school, please follow the Resource Replacement Scheme process.

Insurance excess

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.

Travelling with an NSSCF device

Interstate: Students may wish to take their devices interstate with them, either on school excursions or holidays.

Devices taken interstate will be covered by accidental damage protection (see the Damaged devices section of this document), however if the device is lost or stolen while interstate the cost of replacement will be covered by the NSSCF program (excesses will apply).

Processes for stolen or damaged devices still apply the same as if they were in Queensland.

International: Students may be approved to take their device overseas but the following applies:

- Permission must be given by the principal (this permission should be recorded in OAMPS)
- Parents should be advised to include the student device in their own travel insurance policy
- Schools should retain verification of permission and parental insurance policy for their records
- Accidental damage cover and warranty will not apply overseas.

Damaged devices

Bulk purchased Acer Aspire 1830T devices include a comprehensive four-year warranty. The warranty period starts when the device is received at the school.

Warranty and service request details

Item	Details
Support vendor	Acer Australia
Contact number	1800 819 713 (only available to school staff, parents or caregivers)
Operating hours	Phone logging: 7am – 8pm, Monday to Friday Website address: site currently under construction
Information required to log a request	Contact name (school or parent) Contact number Device serial number (SNID) Email address (for online logged requests) School or home location (address) Request details (i.e. description of the fault)

Accidental damage cover

The department has negotiated an accidental damage cover to support schools and families when a 'genuine accident' results in damage to a device (excesses will apply). Examples of accidental damage are:

Type of damage	Examples of damage
Accidental liquid spill damage	Accidentally spilling liquid over the keyboard
Unintentional impact damage	Accidentally dropping the notebook, which results in physical damages to it
Electrical surge	Blackouts or storm surges
Accidental breakage	Broken AC power pins

Accidental damage warranty related costs

The excess charged to the school is shown below:

Occurrence	Cost
1st	$50
2nd	$100
3rd	$150
All subsequent incidents	$150

Parental costs incurred are a school managed process.

It is suggested each school sets up an invoice system in NSSCF

Device fault data listed is provisional only.
Faults are reconciled by the hardware vendor monthly, and are subject to change.
The final determination of warranty coverage is made by the hardware vendor.

Non-warranty damage

Non-warranty damage is where damage is not covered by warranty and not classified as accidental damage.

The Acer warranty does not cover the device for any wilful damage, carless damage or theft. Examples of items not covered are:

Type of Damage	Examples of damage
Non-warranty damage	Any keys being removed from the notebook's keyboard due to excessive force applied.
Non-warranty damage	Leaving objects (such as pens) on the keyboard when closing the notebook lid, and as a result the LCD display is damaged.
Non-warranty damage	Leaving the notebook unattended and as a result it was damaged by someone or something else other than the user or assigned owner.
Non-warranty damage	Repeating cases for the same Notebook which may have previously been termed as accidents.

Non warranty claims may lead to a school reconsidering participation in take home programs.

Occurrence	Cost
Repair, excluding repair or replacement of LCD screen	$147 excluding GST
Repair, including repair or replacement of LCD screen	$257 excluding GST
Intentional 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.

Parental costs incurred are a school managed process.

Device fault data listed is provisional only.

Faults are reconciled by the hardware vendor monthly, and are subject to change.

The final determination of warranty coverage is made by the hardware vendor.

Multiple failures

For NSSCF Q3 bulk purchased devices, Acer provides a multiple failures service or ‘lemon clause’. The details of this clause are shown below:

Policy	Conditions
1	During the warranty period, Acer will replace and deliver, at no cost to DET, any NSSCF Q3 device on the occasion of that products third claim under warranty. Replacement of the device only applies for the first three years of the warranty period.
2	The device replaced under this program will be the current equivalent model of the failed product. If that failed device has been superseded the current model will be provided, this will include the balance of the original warranty on a pro-rata basis. The replacement product will include all the components originally ordered with the failed product, including DET’ s managed operating environment (MOE) Acer will ensure the replacement device will be received at the relevant School within five school days, or as agreed with Acer, from the date the claim was made to Acer.

Help and support

DET has bulk purchased Acer devices that have a lifecycle of four years and meet the technological requirements of students from Years 9 to 12.

Technical support will be provided directly by Acer. In most cases, Acer will supply next day on-site support. In some remote locations, the device may be required to be returned to Acer.

Logging a service request with Acer

All requests are logged directly with Acer.

There are two methods by which to log service requests. They are:

- by phoning 1800 819 713
- logging a job online – site currently under construction

Phone requests can only be logged by school staff or parents. Students under the age of 18 will need to ask their parents or someone at school to log a service call for them. The staff in the Acer help centre have not undertaken a working with children check.

Please note: the Acer service centre is only available for DET-owned Acer devices. All DET hardware information is available to the vendor to ensure devices are DET owned. Personal devices are not supported within this support service model.

Data Storage

School managed processes

File system quotas

An administrator can specify warning and limit thresholds on the amount of disk space at the folder (and volume) that a user can consume as well as screening of file types and storage reports. This setting can be modified by contacting the Service Centre 1800 680 445.

Quotas will be left to the discretion of each school to set up and manage.

Redirected folders

By default, there are a number of redirected folders utilised via Group Policy.

These folders will be directed to the local D:\ on the device and are as follows;

- My Documents (My Pictures, My Videos, My Music)
- Application data
- Userhome folder (downloads, favourite, links, saved games, searches, documents, contracts).

As all user data is stored locally on the device, it is the responsibility of the device owner to ensure appropriate, regular backups are performed on suitable external media.

Back up responsibilities

The importance of backing up data stored on devices cannot be over-emphasised.

Students are encouraged to back up their data using an external device at least once a week. This will minimise disruption caused by virus damage or hardware failure.

Please remember that hard drives can fail. Students with devices that suffer from hard drive failures may lose all files stored on their computers.

Saving data to the network

Data can be saved to the school's usual network locations such as the H: drive, which are managed by school back up procedures.

You will need to consider any quotas you have at your school and the possible impact the amount of data being saved to these locations may have.

This will also render the data unavailable when not working within the school environment.

Saving data to USB media

The easiest way to back up files is to use a USB drive. If a USB drive is being used as a backup medium, it is strongly recommended this be made the sole purpose and the USB stored securely away from the device.

Windows backup (fortnightly image)

As part of the Q3 build, Windows 7 will provide a prompt to back up the device's C: drive once a fortnight if power is plugged into the device. To perform a back-up, the 'OK' button must be clicked on this prompt. This process will back up the C: drive to an image on the D: drive.

If the timing is inconvenient then the prompt can be left in the background while continuing to work on other items, allowing the option to perform the back up at a more convenient time. The power needs to be plugged into the device for the back-up to be performed.

Students with devices that suffer from hard drive failures may lose all files stored on their computers, including this back up image on the D: drive. To alleviate this concern the D: drive can be copied to an external source, such as a USB drive.

Allocation and Management

Opt-in devices provided to your school within the National Secondary Schools Computer Fund Q3 allocation will be issued with device project names and numbers. These are generated in the Operational Asset Management Provisioning System (OAMPS) by the NSSCF Project Team and workstation names are initiated during the automated workstation joiner process.

This means any Opt-in devices in OAMPS require no further school asset data entry.
For further information regarding OAMPS, please view the OAMPS guide on the NSSCF Q3 Rollout Community team site.

Asset Labelling

All NSSCF Q3 devices will be asset labelled as NDL12345, where the number is unique to NSSCF round Q3 devices. The NSSCF asset label (Project ID) will be generated and attached to the device by the vendor for any devices supplied via the NSSCF program Q3 bulk purchase (i.e. the Acer Aspire 1830T with 3G data plan and accidental damage warranty).

If your school needs to label an Opt-out device with an NSCCF asset number, please contact the project team at NSSCF-Q3@deta.qld.gov.au. NSSCF Administration will provide you a block of asset numbers as per your outlined requirements and maintain a central listing of these until such a time as the functionality to self-manage this, while maintaining a unique asset number between all schools, is made available within the OAMPS.

After you receive the spread sheet from NSSCF Administration containing the block of NSSCF asset numbers, you will need to register the workstation name by adding the last 5 digits of NDLxxxxx to your school prefix after the NDL, ie NDL1234xxxxx. This will ensure successful registration of your Opt-out (alternative devices) in Active Directory.

The NSSCF asset number sheet provided to you is determined by how many devices are Opt-out and will look like this:

Site Code	Site Name	Make	Model Number	SNID	Serial Number	Warranty Start Date	Warranty End Date	NSSCF Asset (Project ID)	Active Directory Workstation N	Part Number
1234	Example State High School	Acer	Aspire 1830 3G Model with bag					NDL77356	NDL123477356	AS.18A92.61C2E
1234	Example State High School	Acer	Aspire 1830 3G Model with bag					NDL77357	NDL123477357	AS.18A92.61C2E
1234	Example State High School	Acer	Aspire 1830 3G Model with bag					NDL77358	NDL123477358	AS.18A92.61C2E
1234	Example State High School	Acer	Aspire 1830 3G Model with bag					NDL77359	NDL123477359	AS.18A92.61C2E
1234	Example State High School	Acer	Aspire 1830 3G Model with bag					NDL77360	NDL123477360	AS.18A92.61C2E
1234	Example State High School	Acer	Aspire 1830 3G Model with bag					NDL77361	NDL123477361	AS.18A92.61C2E

Please fill empty fields as completely as possible prior to returning to

NSSCF-Q3@deta.qld.gov.au.

Workstation Name

The NSSCF project computer name will be generated and assigned to the device by the Operational Asset Management and Provisioning System during the automated workstation joiner process for any devices supplied via the NSSCF program Q3 bulk purchase.

For Opt-out and Flexible Funding devices, the workstation name must be entered by the school in the following format:

	National Secondary School Computer Fund	**Round designator** **D – Round Q3**	**Device type (D, L, M or O)** **D – Desktop** **L- Device computer** **M – Computer monitor** **O – Other ICT equipment**	**Location code**	**Asset label number** **5 digit asset number provided by NSSCF project team**
Example	**N**	**D**	**L**	**9999**	**99999**

If you have any questions around the inability to apply a workstation name to a Q3 Opt-out (i.e. an iPad) please contact NSSCF-Q3@deta.qld.gov.au for further information.

Take home devices

A Student NSSCF Charter is provided for schools who wish to have their students sign an agreement before participating in a take-home program.

Included in the Charter is a section for parents to choose the level of elevated access and web filtering they wish their child to have.

Resources are available on the NSSCF Q3 Rollout community to assist schools in running a take-home orientation program.

Maintenance of effort

Schools have a responsibility to maintain effort and investment in ICT to contribute to the one-to-one student to computer ratio for students in years 9-12.

DEEWR used the 2007 census period to determine NSSCF allocations to complete the one-to-one ratio. This means that schools received the correct number of devices they needed to achieve the one-to-one ratio from the baseline ratio of school ownership at that point in time.

Principals and deputy principals can access the NSSCF dashboard to determine their status in relation to maintaining the school fleet. As per the National Partnership Agreement, it is a requirement of the NSSCF for schools to maintain their percentage of the devices that make up the one-to-one fleet. All one-to-one devices need to be maintained