

IMPLEMENTATION ADVICE

In early 2007, the Department of Education and Training released [ICT-PR-004: Using the Department's Corporate ICT Network](#) to provide direction on accessing and using the Department's ICT network, including, intranet, extranet, internet and network access and usage for students and staff, and the publication of personal information to departmental websites.

To assist departmental staff and schools to further implement certain elements of the ICT-PR-004, this implementation advice has been developed covering private device access and the school network usage and access statement/guideline.

Please note, utilising the information contained within this implementation advice does not negate the requirement to be aware of, and adhere to, all elements of ICT-PR-004.

1.0 Private Device Access

ICT-PR-004 was developed through the amalgamation and updating of a number of existing policies, but also included a new section to provide a policy structure for private device access to the Department's corporate ICT network. While the Department reserves the right to restrict access of privately owned ICT devices, there is awareness that limited private device access is essential for the effective running of business units and schools. However, this must be balanced with appropriate safeguards being employed from managerial level through to learners and teachers.

1.1 Managers/Principals - Essential considerations for approving staff private device access:

Managers and Principals must ensure the following protocols are in place prior to approving staff and teachers private device access to the corporate ICT network:

- Laptops: must be configured according to the Department's corporate standard operating environment to meet the requirements of encryption, authentication and security locking including session time-outs. At a minimum, the device should have encryption and virus protection software regularly updated with the latest virus definition files, and some form of firewall.
- Mobile Wireless Assistants (PDAs): the device should be configured with encryption software, authentication system (e.g. password locking) and a security locking mechanism including session time-outs.
- All private devices are to be operated only in areas where the security of the information can be assured.
- Network connections of all privately owned devices will be cancelled upon termination of employment and can be revoked at any time based on due cause (e.g security breaches, investigation).

Managers and Principals, prior to or after approval is given, suspecting private devices are not meeting network security and operational requirements should ensure restriction of access to maintain the integrity of the corporate ICT network.

1.2 Student Private Device Access

The departmental position remains that schools should ensure students do not connect solely privately owned ICT devices to the Department's corporate ICT network, due to the level at which such mass access would compromise the integrity of the corporate network.

The Department will reassess its position with the release of the Network Access Protocol (NAP), where additional functionality could provide the ability to control the level of access student private devices on the corporate network.

1.2.1 USB Flash Drives

While USBs fall under the definition of private devices, it is acceptable that schools allow student's to use such devices to fulfil their educational program requirements (e.g. bring assessment items to school as opposed e-mailing).

However, schools should ensure that appropriate virus scanning occurs on all files downloaded to the corporate ICT network and students should be advised on appropriate security practices (e.g. virus scanning before removing file from home computer and again on download to corporate network, advising teacher/supervisor as soon as any breach of security is suspected).

Caution should always be employed with the use of USBs, particularly as the capacity of these devices to store a large number and size of files continually increases due to technology advancement.

1.3 Conclusion

If in doubt when implementing protocols around the management of private device access on the Department's corporate ICT network, further advice can be sought from the Service Centre, ph: 1800 680 445, on the technical requirements for private device access.

Additionally, your Regional Technology Manager, contactable through your local Regional/District Office, can provide advice on implementation within the school environment.

A major element of the success of managing private device access lies in the appropriate operation of such devices and usage of the corporate network by all users. Reporting of suspected or detected security incidents, to the Manager, Information Security (via the [Information Security Incident Reporting Form](#) - For Internal Use Only), should be undertaken as soon as major breaches occur.

2.0 School network usage and access statement or guideline

ICT-PR-004 provides direction to school Principals around formulating a school network usage and access statement or guideline and ensuring school staff, students and parents understand, acknowledge and sign the guideline/statement.

The implementation of this provision was defined to allow Principals the flexibility to implement the requirement to suit individual school operations. The main requirement allows for Principals to either seek sign-off on enrolment of students or employment of staff. Alternatively, sign-off could be sought at the start of each school year.

Since release of ICT-PR-004 some schools have provided feedback that further guidance on the major elements to be covered in the school network usage and access statement/guideline is required. Following are dot points to assist schools with the formulation of the statement/guideline:

2.1 Key Sections Key Messages

2.1.1 Purpose Statement:

- ICT, including access and use of the internet, are essential tools for schools in the provision of innovative educational programs.
- Schools are constantly exploring new and innovative ways to incorporate safe and secure ICT usage into the educational program.
- Further guidance on drafting this section can be sought from the [Information for Students and their Parents](#) information sheet (Why are schools providing students access to ICT facilities?) and the [Information for Staff using the Department's ICT network](#) information sheet (Why are staff provided access to ICT facilities in the workplace?).

2.1.2 Responsibilities:

- Principals and teachers have main responsibility to ensure adherence to policy for the safe and effective use of ICTs within schools.
- Staff and students also have responsibility to ensure they employ appropriate behaviour when using the school's ICT network.
- Parents/guardians are responsible for conveying and ensuring students understand the schools ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements. Further guidance on drafting this section can be sought from the [Information for Students and their Parents](#) and the [Information for Staff using the Department's ICT network](#) (Can a staff member use the departmental network for personal use? Inappropriate Use) information sheets.

2.1.3 School Monitoring:

- The school and the Department will monitor the access and usage of the ICT network. For example, e-mail monitoring will occur to identify inappropriate use, protect system security, maintain system performance, determine compliance with State and departmental policy and determine compliance with State and federal legislation and regulation.
- Schools reserve the right to restrict staff or student access to network services if access and usage requirements are not met or breached.

- However, restricted access should not disrupt the provision of the educational program within the school. For example, a student with restricted school network access may be allocated a stand-alone workstation to continue educational program activities.
- Further guidance on drafting this section can be sought from the [Information for Staff using the Department's ICT network](#) and the [Information for Students and their Parents](#) information sheets.

2.1.4 Private Device Access:

- While staff may seek approval from the Principal for limited private device access, it should be made clear that students are not permitted to connect solely privately owned devices to the network.
- Further guidance on drafting this section can be sought from the [Student Private Device Access](#) implementation advice provided in this document.

2.2 Consultation

Schools are encouraged to undertake consultation with the school community when developing or reviewing the school network usage and access statement or guideline.

2.3 Availability

Staff, students and their parents/guardians should be provided with a hard copy of the statement/guideline for signing. Additionally, the statement or guideline should be made available on the school's website and form part of the communication undertaken within the wider school community.

2.4 Sign-off

The implementation of the sign-off process for school staff, students and their parents/guardians can occur on enrolment/employment or through an annual collection, whichever suits the school's normal operations. The following is a suggested format for the signature block to be placed at the end of the statement/guideline:

2.4.1 Staff member:

As part of my employment with the school, I understand and will adhere to the school's network usage and access statement/guideline and the Department of Education and Training [ICT-PR-004: Using the Department's Corporate ICT Network](#).

I understand that should I be involved in a breach of either the schools' network usage and access statement/guideline or the Department of Education and Training [ICT-PR-004: Using the Department's Corporate ICT Network](#), the school may decide to restrict my access to its network and, if deemed a security breach to the network, may be reported directly to the Department.

_____ (Staff member's name)

_____ (Staff member's signature) _____ (Date)

2.4.2 Student:

I understand that the school's ICT network provides me with access to a range of essential learning tools, including the internet. I understand that the internet can connect me to useful information stored on computers from around the world.

While I have access to the school's ICT network: I will only use it for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.

Specifically in relation to e-mail and internet usage, I will: clear any offensive pictures or information from my screen; and immediately quietly inform my teacher. In the same instance I will not: reveal home addresses or phone numbers – mine or that of any other person; or use the school's ICT network (including the internet) to annoy or offend anyone else.

I understand that if the school decides I have broken the rules for using its ICT network, appropriate action will be taken, which may include loss of access to the network (including the internet) for some time.

_____ (Student's name)

_____ (Student's signature) _____ (Date)

2.4.3 Parent or Guardian:

I understand that the school provides my child with access to the school's network (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information on computers from around the world; that the school can not control what is on those computers; and that a small part of that information can be illegal, dangerous or offensive.

I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend finally upon responsible use by students/my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT network.

I believe _____ (name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT network (including the internet) under the school rules. I understand that students breaking these rules will be subject to appropriate action by the school. This may include loss of access and usage of the school's ICT network for some time.

_____ (Parent/Guardian's name)

_____ (Parent/Guardian's signature) _____ (Date)