Rous Public School

Information Communication Technology

Policy Document

Contents

DEFINITION

Information and Communication Technology (ICT) means all computer hardware, software, systems and technology (including the Internet and email) and telecommunications devices and facilities that may be used or accessed from the school or connected to a school's communication network.

RATIONALE

Rous school believes that we must completely equip the children of the 21st century with the skills, knowledge and understanding, which will guarantee their active participation in a technological age.

AIMS

Rous school values an education which develops life skills for children, enabling them to appropriately interact socially and academically.
Therefore the ICT programme offered at our school aims to develop children who are :

- competent and creative with information & communication technology;
- independently using higher order thinking skills;
- able to collaborate and communicate with a wide range of learners in a varied settings;
- citizens who contribute positively and who are sensitive to the evolving social and ethical values of the community.
- competent in learning & using language in a broad range of contexts.

IMPLEMENTATION

The ICT policy involves the following personnel:

- Teachers including Teacher-Librarian and Teacher aides
- Parents and helpers who use the school computers
- Office personnel

Procedures

The ICT program will the follow NSW DET supporting documents based on the K-6 Syllabii for all KLA's:

- ICT Acceptable Usage Program
- Digital Image Agreement
- K-6 ICT Scope and Sequence
- Staff Development opportunities

Assessment

Children in year 6 will participate in the Computer Basic Skills Test each year.

EVALUATION

The evaluation of this ICT policy will take place

- every 3-4 years or
- as the need arises
- when changes in curriculum occur

This will be done by:

- ICT committee teaching staff
- staff meetings and/or policy review meetings

ICT Committee

Representative group of staff

The ICT committee will include the Principal, Computer Co-ordinator and Senior Administration Officer (SAM). In the absence of a Computer co-ordinator the Principal may nominate a member of staff who has some knowledge of ICT issues to the representative group.

Role of committee

The role of the committee is to consult with staff and parents and/or community members, professional bodies and DET personnel in the advancement of ICT use and objectives within the school. The committee will be responsible as a group or as an individual for:

- Software
    - Reviewing/recommending software
    - Purchasing of software
    - Installing software
    - Dealing with problems that arise with the software
- Hardware
    - Reviewing /recommending hardware
    - Purchasing or ordering hardware
    - Adding hardware (unless DET personnel responsibility)
    - Dealing with problems that have arisen with the hardware
- Internet and Network
    - Maintain Internet and Network connections
    - Refer Internet /Network to ICT Help desk if can not be addressed by Computer-co-ordinator
    - Ensure DET guidelines are followed as to use of Internet
    - Deal with any issues or problems that have arisen from the improper use of the internet
- Security
    - Ensure that all computer hardware/software is held in a secure environment
    - Ensure that Wireless Internet connections are secure at all times
    - Maintain a secure Network environment and advise DET ICT help if any unusual activity has occurred.
    - Ensure that up to date virus protection is on all computers.

ICT Administration

The role of the computer coordinator

The computer co-ordinator has the role as both advisory and management of ICT issues. The computer co-ordinator will, by virtue of their position and expertise, be involved in most of the day to day management, running and maintaining of the computer fleet (whether in the classroom, lab or in the administration /principal's office).

Management includes:

- Trouble shooting any minor computer problems
- Advising any problems that can not be fixed to ICT help desk
- Maintaining computer updates and virus protection
- Ensuring all computers are working in a reasonable manner

- Advise of any purchases to committee for maintaining working fleet
- Provide recommendations for T4L purchases
- Regularly perform defragment and clean-up of hard drive
- Regularly perform clean up of My Documents and student folders

Regional ICT team.

The computer co-ordinator must maintain reasonable contact with the local DET ICT team. Most issues that arise with the DET computers will referred to the ICT help desk 1800 338 834. A case number will be issued whereby the problem must be followed up by the ICT team.

When possible and at the discretion of the Principal the computer co-ordinator should attend any in-service/conference or seminars to be aware of DET policies. At all times the computer co-ordinator should be aware of any upcoming proposals and policies set out by the DET and should not obtain hardware or approve infrastructure without consultation with the regional ICT team.

It is at the computer co-ordinators and principals discretion to obtain the services of a private computer company to address minor improvements or repair any equipment that falls outside of the DET computer fleet. These services must be paid from school funds.

DET Policy and Procedures

Code of Conduct

Computing facilities are provided primarily for the educational benefit of students and the professional development of staff. We want all our students to recognise and realise the full potential of this new medium and become productive members of a future society in which computers will become an increasingly important component. The School will provide training for students in computing and internet use, and also will make users aware of the School Computer Policy. Behaviour that interferes with these primary objectives will be unacceptable. The code of conduct includes all users at NSW Public School computer networks and also applies to the use of any of the School owned computers, wherever they are physically located. The acceptable usage policy can be viewed in Appendix 1

Internet Access

Is available to assist students with their education. Filtering software is in place on all departmental computers. In the end however it is the responsibility of individual students to ensure that material they view is appropriate. Violent games and games that require considerable bandwidth will be discouraged (See Appendix 1)

File Storage

Although the school makes every effort to ensure the integrity and back-up of data on the School network, users are advised to ensure they have a second copy (backup) of all their academic data.
All pupils have document storage areas and an email account on the fileserver. In addition, Shared Work group namely the “h” drive areas are available on the servers. Any files which are deliberately stored on the servers in an area contrary to its intended purpose may be deleted without notice by the computer co-ordinator and/or Principal.

Use of Podcasts/Videos and DVD's

Podcasting in schools

The objective and intent of this policy is to provide information to schools on copyright issues related to Podcasting.

Audience and applicability

This policy applies to all staff and students in NSW government schools.

Context

This policy has been developed in accordance with the *Copyright Act 1968.*

Responsibilities and delegations

Before downloading or viewing a podcast staff in schools should check the podcasters terms and conditions and ensure they are permitted to use the podcast for 'educational purposes'.

When a school is creating their own podcast they are required to:

- obtain permission for the use of any material included in the podcast such as music tracks or films owned by another person
- obtain written consent of students (or parent/guardians) and other persons appearing in a podcast

When creating a podcast and using externally owned copyright material schools will generally be required to "credit' (acknowledge) the copyright owner in the final product as part of the licence agreement.

Copyright: Screening pirated DVDs in schools

Information to all schools on screening pirated DVDs.

The objective and intent of this policy is to provide information to schools on how to avoid owning or screening pirated DVDs.

Audience and applicability

Applicable to all staff and students in NSW government schools.
This policy has been developed in accordance with legislative requirements set out in the *Copyright Act 1968.*
Under the *Copyright Act 1968* it is a criminal offence to possess or screen films that have been pirated or copied illegally. Allowing pirated DVDs to be screened on school premises puts schools, principals, staff, parents and students at risk of criminal prosecution for DVD piracy.
Schools principals should ensure that staff, teachers and students are made aware of the risks surrounding piracy and only screen DVDs obtained from legitimate sources.

Responsibilities and delegations

Each school is responsible for ensuring that they do not possess or screen films that have been pirated or copied illegally.

FILMS, VIDEOS, DVDs AND COMPUTER GAMES IN SCHOOLS

Classification of films and computer games

The National Classification Scheme (NCS) is a cooperative arrangement under which a Classification Board classifies films (including videos and DVDs), computer games and certain publications on behalf of the States and Territories. The Scheme commenced in 1996 and is administered by the Office of Film and Literature Classification (OFLC).

Under the National Classification Scheme, the States and Territories are responsible for the enforcement of classification decisions. Therefore, each State and Territory has classification enforcement legislation to

complement the Commonwealth Classification Act. The New South Wales legislation is the *Classification (Publications, Films and Computer Games) Enforcement Act 1995.*

In general, films and computer games are classified as **G, PG, M** and **MA 15+**. Films may also be classified **R 18+**. G, PG and M are **advisory classifications** recommending the appropriate audience. MA 15+ and R 18+ are **legally restricted categories.**

Directions for Schools
All films and computer games must be previewed by teachers prior to use with students. The reviewer should give particular consideration to the suitability of the material in the educational context and the age and maturity of the intended audience. The use of classified films and computer games in schools requires the approval of the Principal. The Principal may delegate the approval of the use of G and PG material to an executive member of staff but must not delegate approval relating to M and MA 15+ material in Primary classes.

Material classified PG should only be used with students after careful consideration by teaching staff who should recognise that material in this classification might upset, frighten or confuse some students. Staff may wish to inform parents in advance of presentation so that they may be given the opportunity to withdraw their child from the viewing.

Digital Images

Photos and Videos may be taken of your child and sometimes other family members during school activities. These may be placed in such places as: the notice board, School Website, Intranet, school assignments, end of year presentations, orientation, class projects, school newsletter, the local newspapers. It is at the discretion of the parent whether do or do not permit photos of their child to be published see Appendix 2

ICT Funds

Computer Coordination

Funds are held in accordance DET guidelines for the role of computer co-ordinator and the co-ordination of the technology KLA. The administration, delegation and payment of those funds is controlled and monitored by the Principal and SAM.

Grants

Where possible the computer committee and/or Principal should actively seek funding for computer/technology grants. Grants in the form of the T4L program, take back program and other initiatives should be constantly considered. The computer co-ordinator may advise the computer committee of the best or appropriate choices for purchase.

Payments

Priority must be given to salary for computer co-ordinator and/or other related salary payments. Funds then will be considered or regarded for payment for in-servicing/training of the computer co-ordinator.

Any other additional funds will be used for purchase and/or payments for goods and services such as:

- software
- hardware
- maintenance/repairs
- improvement/upgrading
- wireless access (and associated running costs)
- miscellaneous and unexpected costs

ICT Standards

Computers and Servers

Each school has an allocation of T4L computers along with computers purchased from sources such as the procurement services, local business and/or private donations. Preference for Mac/Apple or PC is the responsibility of the School computer committee. The majority of computers are PC.

The servers supplied by the DET and installed by their technicians and serviced by their technicians are predominantly PC. T4L computers are predominantly PC

Printers

Printers vary according to needs and may be part of the existing hardware within the school or purchased from local businesses. Printers may also include Multi-Function devices which includes copy/scan and fax abilities. Printers can be laser/ink cartridge black ink only or coloured ink.

Printers are used for the following purposes:

- Office administration
- Principal administration
- Teachers use - administrations and/or programming and student work sample
- Students work samples.

Students must obtain permission before printing. No cost is imposed on student work provided it is not excessive. As a general rule colour printing is not provided for students. If the teacher sees fit to allow coloured printing then consideration must be given to the amount of colour on the page and how much ink will be used.

Networking Services

Data Communications

Data communication involves the transmission of data from the original source to another device. In NSW public schools the method of transmitting data may include the following:

- DET intranet
- Oasis
- Fileserver ('H' Drive)

Overseeing of the Data communication is the responsibility of the DET and any problems or breakdowns must be referred to the ICT help desk who will advise of further action.

Fileserver ('H' drive) is not part of the DET service and any measures to obtain, maintain and/or repair will be funded by the school.

Compliance with DET standards

All schools must comply with DET standards if they wish to maintain services and back up and warranty. The compliance includes the computers (currently Lenovo) supplied through the T4L and procurement program. Any computers purchased outside the 'standards' will not be part of the service/back-up or warranty provided by the DET. Therefore payment for purchase, service, repairs and maintenance will be the responsibility of the school.

Whilst it is not mandatory it is advisable to purchase Lenovo or similar PC's for consistency for students , staff and management.

Data Management

Data Security

All staff must follow the DET guidelines when dealing with 'sensitive' data. Records on students and/or staff must be kept secure by way of password protection. Those people with authority to administer the records will ensure that no outside or unknown persons obtain the sensitive or personal data.

Access to staff portal using username and password must always remain unknown to students. If in the event any staff member believes that a student or students have accessed entry to the portal via their username/password and are using it to gain sensitive or unauthorized data they must report this immediately the Principal. Username and password must be changed.

Access to the administration component of the PC's must also follow the above guidelines.

Storage Management

Most information is stored electronically through the thin client/fileserver system as set up by the DET.

Student storage of information (files/documents) on the computers is in either:

- My documents
- Desktop or
- 'H' drive

The computer co-ordinator has the role of providing access to the above storage facility but also has the role of managing that facility. Therefore at the computer co-ordinator discretion s/he may delete old, unused or trivial files to ensure the overall housekeeping of the storage facility.

Backup and Recovery

Back up of administration and library information is performed as a daily (administration) and weekly (library) through the thin client (portal). It is the discretion of the SAM and teacher librarian when the back up is performed and if any additional back ups are warranted.

The DET guidelines and protocol for back up and recovery management will be followed at all times. In the event of major loss of data the Principal, SAM and computer co-ordinator must advice the appropriate personnel and seek instructions for the prompt recovery of data.

Equipment

Client Equipment Fleet Size

Our School currently has the following computer fleet size

__ _ IBM Thinkpad Notebook (Laptops)

___ Lenovo ThinkCentre PC's

___ Thin client

___ Fileserver

Interactive Whiteboards

Schools who have purchased IWB's or similar have done so at their own cost. The connected classroom project will be providing schools with a specific set of IWB hardware that will take the place of previous items. When installed the components of the IWB will be recorded here.

The Current IWB is a portable device which attaches to the digital projector. Funding for this IWB came out of discretionary funds and is serviced (if necessary) through private arrangements.

Printers

Principals Office

Main Office

Classrooms

Computer Room

Library

Other

Password Management

Password Policy

All computers have administration/staff and student access. The access to administration and staff is password protected and must remain unknown to students. Administration passwords must remain school code+local. Staff passwords is at the discretion of the computer co-ordinator.

Student password for computer start up is not required however access to the Portal for internet ccess does require student username and password. The management of the passwords is the responsibility of any computer committee members or classroom teacher. Students in Years 5/6 may manage their own password however access can be gained to change it, if necessary, by the aforementioned. Students are to be advised that their password is 'secret' and must remain that way (see computer use policy)

Security

Physical

All PC's must be secured to the table by DET approved methods. Laptops must be secured either in a trolley or locked room. As an alternative PC's may be secured by placing them in a room which has an alarm system.

Training

ICT Administration Training

Attendance to ICT training for SAM and computer co-ordinator must be considered in view of the importance, relevance, needs and costs for the school. The attendance to such training will be at the discretion of the Principal. Funding will be via the allocated funds or as directed by the Principal.

Appendix

1. Acceptable Usage Policy

General Policies

- Priority will be given to students using computers/internet for educational purposes i.e. research, publication & completion of computer projects, assignments,
- Appropriate use of language must be used in all activities including email.
- Consideration must be given to other computer users, ensuring all users receive equal computer time.
- Sound levels need to be moderated to avoid inconvenience to other users.
- Computers are expensive and sensitive and must be treated carefully.

Students must not

- Attempt to repair hardware without permission.
- Reset computers or change computer preferences.
- Unplug cables or equipment.
- Turn off computers or printers.
- Knowingly infringe copyright.
- Carelessly or deliberately waste resources (all printing must be first approved by the teacher on duty).
- Touch monitor buttons on the front of the computer.
- Fill-in questionnaires or other interactive forms on the Internet without permission.
- Download programs or games.

Students must

- Report other people breaking these rules.
- Follow the teacher's instructions while in the Library using Computers.
- Always close the programs before leaving their computer.

Blocked Sites

The NSW DET uses software to block websites which are illegal or which most parents would regard as inappropriate. Inevitably, not all unsuitable sites will be blocked.

Pupils must not:

- attempt to access inappropriate material such as pornographic, racist, or other offensive material.
- attempt to go on sites such as YouTube, My Space, and Facebook including accessing at home, to post comments about existing and past members of staff or pupils.

Acceptable use of internet and email

This document defines the policy for school students of the NSW Department of Education and Training for the appropriate and acceptable use of Internet and email services provided by the Department.

Policy statement

1.1 The Internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Email communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to email and the Internet in their community. They have the right to expect secure access to these services as part of their learning experiences with the NSW Department of Education and Training.

1.2 Use of the Internet and email services provided by the NSW Department of Education and Training is intended for research and learning and communication between students and staff. Access to Internet and email

at school will assist students to develop the information and communication skills necessary to use the Internet effectively and appropriately.

1.3 Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

1.4 Students using Internet and email services have the responsibility to report inappropriate behaviour and material to their supervisors.

1.5 Students who use the *Internet and Email Services application* provided by the NSW Department of Education and Training must abide by the Department's conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

1.6 Students should be aware that a breach of this policy may result in disciplinary action in line with their school's discipline policy.

Audience and applicability

2.1 This policy applies to all school students located at NSW Government schools who access Internet and email services within the NSW Department of Education and Training network and from any external location.

Context

3.1 This policy document takes account of the Memorandum *Student Access to the Internet* of 18 July 1997 and the Memorandum DN/04/00215 – *Review by Schools of their Student Access to the Internet Policies.* This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies.

Responsibilities and delegations

4.1 Access and Security

Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through Internet and Email Services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal e-learning account.
- log off at the end of each session to ensure that nobody else can use their e-learning account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
    - a message that was sent to them in confidence.
    - a computer virus or attachment that is capable of damaging recipients' computers.
    - chain letters and hoax emails.
    - spam, eg unsolicited advertising material.
- never send or publish:
    - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
    - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
    - sexually explicit or sexually suggestive material or correspondence.

    - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and Internet and Email Services is generally used for genuine curriculum and educational activities.
- Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of the NSW Department of Education and Training.
- ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
- be aware that all use of Internet and Email Services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the Internet or Intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

Students will be aware that:

- they are held responsible for their actions while using Internet and Email Services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access Internet and Email Services.
- the misuse of Internet and Email Services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

Students will report:

- any Internet site accessed that is considered inappropriate.
- any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Training.

Use of electronic communication devices – Mobile Phones - Blogs

Mobile phones may be used before and after school and at the discretion of the Principal.
Mobile phones must be switched off when not in use and kept out of sight. In particular in school, they must not:

- be used to record still or moving images or to record sound without the permission of a member of staff
- be used to send offensive messages which harass, insult or attack others
- be used to access inappropriate websites
- be used as calculators/watches in class

The following points are worth noting:

- inappropriate material, accessed off site, should not be brought into school and shared with others
- the School reserves the right to check the contents of all mobiles brought into school
- students caught using their mobiles inappropriately will have their mobiles confiscated. They will be returned by the Principal only after a suitable period of time has elapsed.

Issues associated with 'Blogging'

Pupils who have set up their own 'Blogsites' – must exercise care about what is written on such sites particularly if mention is made of the School, its pupils and staff.

Student Agreement:

I have read or had the ICT – acceptable Usage policy rules explained to me. I will follow all these rules when I use ICT's at school.

Students Signature: _____

Parent Agreement

My child who has signed above, understands the rules to be followed in using ICT's at school. I have talked to my child to make sure that the rules are understood. I realise teachers and other school officials will try their best to provide only educationally sound material from the Internet for my child and that should objectionable material or information appear by accident, my child will take immediate action to correct the situation. I give permission for my child to use the Internet while at school.

Parent's Signature: _____

Teacher's Signature: _____ Date: _____

2 Digital Images Agreement

Photos and Videos may be taken of your child and sometimes other family members during school activities. These may be placed in such places as: the Foyer notice board, School Website, Intranet, school assignments, end of year presentations, orientation, class projects, school newsletter, the local newspapers.

Please indicate your level of agreement to this.

I give permission for:

My child's image to be used, as described above, without their name. yes no

My child's image to be used, as described above, with first name only. yes no

The images of other family members used, as described above, yes no

without family names.

Signed:_____ Date:_____

or

I do not wish my child's image to appear in any of the ways described above.

Signed:_____ Date:_____