Computer Network Usage Policy

Access

All students have access to the school's computer system by means of a ‘Login Name' and a password.

Responsibilities

Your computer account is your responsibility. You should make yourself familiar with the school's computer policy (this document). Your account will be disabled for non-observance of the rules set out in this policy.

Password security

Do not tell other students your password. If they can use your account, they can:

- Delete your work
- Copy your assignments
- Act in a way to have your account disabled

Password changes

Passwords can be changed by the computer coordinator or his representative. This will occur after a ‘password request application’ has been obtained from the front office or library and completed.

Printing

To print a document, you must have permission from your class teacher, who will ensure that the printer and paper are available.

Personal laptop computers

Students may connect to the school network only after they have demonstrated to the computer coordinator or his representative that their anti-virus software is up to date and their computer is virus free.

This can be done via cable or wirelessly where a connection is available.

Internet and email

Access to the Internet (via the DET Intranet) is a privilege, not a right. By default all students and staff have internet (and email) access. Your parents may stop this access should they so wish. More detail concerning internet usage is attached.
Woodenbong Central School Internet and email: Acceptable Usage Policy
[To be read in conjunction with school policy on mobile phones and cyber-bullying]

1. Objectives - 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. Online communication links students to provide a collaborative learning environment and is intended to assist with learning outcomes. Today’s students are exposed to online communication tools 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 online communication 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 online communication tools 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 online communication services have the responsibility to report inappropriate behaviour and material to their supervisors.

1.5
Students who use the internet and online communication services 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 Woodenbong Central School’s Welfare and Discipline policy.

2. Context

2.1
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.

2.2
This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies.
3. Responsibilities and delegations

3.1 Access and Security

3.1.1 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 online communication 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, e.g. 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 online communication 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 online communication services can be audited and traced to the e-learning accounts of specific users.

3.2 Privacy and Confidentiality

3.2.1 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.
3.3 Intellectual Property and Copyright

3.2.1 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.

3.4 Misuse and Breaches of Acceptable Usage

3.4.1 Students will be aware that:
- they are held responsible for their actions while using internet and online communication 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 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.

4. Monitoring, evaluation and reporting requirements

4.1 Students will report to their teacher:

4.1.1 any internet site accessed that is considered inappropriate.

4.1.2 any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education and Training