

**STUDENT COMPUTER/INTERNET USE AGREEMENT
NEW PLYMOUTH SCHOOL DISTRICT #372
NEW PLYMOUTH MIDDLE SCHOOL**

SECTION I

I, _____ agree to the following conditions for use of the computer and information network services of New Plymouth School District #372:

I understand and will abide by this district's Information Network Service Acceptable Use Policy. Should I commit any violation of the policy, my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

SECTION II

I further agree to the following specific conditions for the use of New Plymouth's computer and information network service:

1. Copying software is illegal and is prohibited.
2. No beverages may be brought into the computer work area.
3. Playing computer games is not allowed without first obtaining teacher permission.
4. Work is to be only on tasks assigned by the teacher.
5. Any alteration of software is prohibited.
6. Any tampering with hardware or peripherals is vandalism and will be dealt with accordingly.
7. No floppy disks are allowed without prior teacher approval.
8. Security procedures will be followed as outlined by the teacher.
9. Sharing student accounts is prohibited.
10. Privacy of other users will be respected. Electronic "snooping" is not allowed.
11. Community standards of decency will be respected.

I understand that the use of information network services is a privilege and not a right. I also understand that failure to abide by the conditions set forth in this agreement will result in any one of the follow consequences:

- Temporary suspension of computer privileges.
- Suspension of all computer use privileges.
- Referral to appropriate disciplinary and/or legal authorities. (See attached Idaho Code "Computer Crime")

This consent shall be valid unless and until revoked in writing by the undersigned

User Name (please print): _____

User Signature: _____ **Date:** _____

PARENT OR GUARDIAN (If you are under the age of 18, a parent or guardian must also read and sign this agreement.)

As the parent or guardian of _____, I have read this district's Information Network Service Acceptable Use Policy. I understand that this system is designed for educational purposes and that the district has taken reasonable precautions to eliminate controversial material; however, I also recognize it is impossible for the district or school to guarantee that my child will never be exposed to such, and I will not hold the district responsible for exposure that is beyond the district's reasonable control. I accept responsibility for all supervision of my child's use of similar systems when such use does not occur at school. **I hereby give permission** to issue an account for my child and acknowledge that the account may be revoked and disciplinary action taken if my child does not abide by the acceptable use policy.

Parent or Guardian (please print): _____

Parent or Guardian signature: _____ **Date:** _____

ONLINE USE

All school policies and rules pertaining to behavior in communications and the use of electronic media in the classroom apply. The use of New Plymouth's information network services must be for educational purposes only and be consistent with this District's mission.

1. Use may not be for private or commercial purposes. Users shall not attempt to sell or offer for sale any goods or services that could be construed as a commercial enterprise.
2. Illegal activity is prohibited.
 - (a) Sending, receiving, or accessing obscene or pornographic material is prohibited.
 - (b) Sending, receiving, or accessing harassing or objectionable material is prohibited.
 - (c) Violating copyright provisions and laws is prohibited.
 - (d) Using programs to infiltrate a computing system and/or damage the software components is prohibited.
 - (e) Students and staff shall use the information network service resources efficiently to minimize interference with others. Playing computer games or other recreational computer use is not allowed without teacher permission.
 - (f) The systems operator does a complete system backup of information daily; however, individual users are responsible for the security of their own work and should arrange for any necessary additional backups.
 - (g) Users are responsible for taking precautions against computer viruses on their own systems and New Plymouth's systems

STUDENT SAFETY

1. It is the responsibility of all professional employees and school staff personnel to observe student Internet use and to promptly report any activity that could jeopardize the personal safety of any student.
2. Student Internet users may not reveal personal information to anyone on the Internet. Identification must be limited to no more than the identification provided by the system itself. Personal information such as home address, telephone number, personal name, or any other information may not be revealed without first obtaining permission **for each occurrence** from their teacher or professional staff member in charge of the workstation they are using.
3. Student users will not participate in any "chat" activity without first receiving permission **for each occurrence** from the teacher or professional staff member in charge of the workstation they are using.
4. Student users will not agree to meet with someone they have "met" while using any information network service, including but not limited to the Internet.
5. Student users will promptly disclose to their teacher or other professional school employee any message or material they receive or observe that is inappropriate or makes them feel uncomfortable.

ONLINE CONDUCT

All users are expected to abide by the generally accepted rules of computer network service etiquette. These include, but are not limited to the following:

1. Users may not be abusive in their messages to others. Community standards of decency will be respected.
2. Users may not swear, use vulgarities, or any other inappropriate language.
3. The information network service may not be used in such a way that usage would disrupt the use of the network service by others.
4. All communications and information accessible via the information network service should be assumed to be private property but open to school district scrutiny.
5. No user may upload, download, or install software into any district system except by permission of authorized support personnel.
6. User shall not transmit materials, information or software in violation of any local, state, or federal law.
7. Users shall not submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material; nor may they encourage the use of controlled substances.
8. All users must respect privacy of others. Electronic "snooping" is not allowed.
9. Attempts to login to the system using another user's account shall result in termination of the offender's account. No user may attempt to gain unauthorized access to any computer network service or facility, nor attempt to go beyond any authorized access. This includes attempting to login through another person's account or to access any other person's files. These actions are illegal, even if only for the purposes of browsing.
- 10. A user that shares his/her account an/or password with any other person may lose the right to system access and use.**

Any action by a user that is determined by the designed administrator to constitute an inappropriate use of New Plymouth's information network service is strictly prohibited and will result in disciplinary action.

COPYRIGHTED MATERIAL

Copyrighted material and “Shareware” material shall not be placed on any system connected to New Plymouth’s information network service without the author’s written permission. The following shall apply to copyright and “Shareware”, Materials:

1. Only persons specifically authorized to do so may upload such material to the information network service.
2. Users may download only that material for which permission has been requested and granted, or that falls within the fair use exception to the copyright laws.
3. A user may redistribute such material only with the express written permission of the owner or authorized person or as provided by the fair use exception.

ELECTRONIC MAIL

Electronic mail (“Email”) is a private electronic message sent by or to, a user in a correspondence with another person having Email access. The following provisions apply to Email:

1. Messages received by the information network service are retained on the system until deleted by the recipient.
2. A canceled information network service account will not retain its Email access.
3. Users are expected to remove old messages in a timely fashion. The system administrators may remove such messages if not tended regularly by the users.
4. Users should recognize that others might view Email. There is no guarantee of confidentiality.
5. The systems administrators will not intentionally inspect the contents of Email sent by one user to an identified addressee, or disclose such contents to other than the sender, or an intended recipient, without the consent of the sender or an intended recipient, unless required to do so by law or by policies of this district, or to investigate complaints regarding Email which are alleged to contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
6. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any Email transmitted on this district’s information network service.

THIRD PARTY SUPPLIED INFORMATION

Opinions, advice, services and all other information expressed by students, staff, information providers, service providers, or other third party personnel on the information network service provided by this district are those of the individual and do not represent the position of this district.

DISK USAGE

The system administrators reserve the right to set quotas for disk usage on the network system. Users exceeding their quota will be required to delete files to return to compliance. Users may request that their disk quota be increased by submitting a request stating the need for the quota increase. In determining whether to grant the request, the designated administrator shall review the space available and the reason for the request. A user who remains in noncompliance of disk space quotas after (7) days of notification will have their files removed by a system administrator.

SECURITY

Security on any system is a high priority. All users shall meet the following requirements:

1. If a user feels that he/she can identify a security problem on the information network service, the user shall notify a systems administrator. The user shall not demonstrate the problem to others.
2. **Users may not let others use their account and password, nor shall they leave a workstation unattended while it is open to their account.**
3. Users shall change passwords regularly, using combinations of letters and numbers and shall avoid using standard English words and names.
4. Users shall immediately notify a systems administrator if their password is no longer secure, or if they have reason to believe that someone has obtained unauthorized access to their account.
5. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the information network service.

NEW PLYMOUTH SCHOOL DISTRICT #372
INFORMATION NETWORK SERVICE
ACCEPTABLE USE POLICY

GENERAL

New Plymouth's Information Network Service provides an electronic highway connecting millions of computers around the world as well as each of the computer workstations within our district. Students and staff can access information and news from educational and research institutions, send and receive electronic mail (Email), take part in distance learning activities, consult with experts, and view library holdings.

Internet access is part of this service provided by the New Plymouth School District. The system administrators of the Information Network Service are employees of this District and reserve the right to monitor all activity on the network. On acceptance for usage of the Information Network Service, students and staff will be given a user account and password that will be used to control and monitor access. This account and password must not be shared with any other person.

Users may encounter information on the Internet and other information services that may be perceived as controversial or potentially harmful. New Plymouth cannot control the Internet and other network sources of information, but the District will strive to provide students and staff with the understanding and skills needed to use information network services in an appropriate manner.

STAFF USE

This use policy is intended to apply to all users of the District Information Network Systems. Wherever appropriate, provisions apply to staff as well as students.

PRIVILEGES AND RESPONSIBILITIES

1. The use of New Plymouth's information networking capabilities is **a privilege, not a right**. Permission from parents or guardians is required before students may access network services. All school district users must sign an acceptable use agreement before access is permitted.
2. Student and staff freedom of speech and access to information will be honored; however, this school reserves the right to monitor and review all the electronic transmissions and activities. Access may be denied, revoked, or suspended to specific users at anytime because of inappropriate use. Further disciplinary action may also occur.
3. **Use of New Plymouth's information networking capabilities must be directly related to education consistent with the instructional objectives of this District.**

INFORMATION CONTENT

New Plymouth School District provides students and staff access to other information systems around the world through the Internet. This District and its administrators do not have control of the content of information that may be found in all other information systems. Some information systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening racially offensive, or illegal materials. The New Plymouth School District does not condone the use of such materials and does not knowingly permit use of such materials in the school environment. Parents of students should be aware that such materials exist. Students bringing such materials into the school environment will be dealt with according to the discipline policies of the individual school building and this district. Intentionally accessing or using such materials will result in termination of access to New Plymouth's computer and information network services and may result in in-school suspension, suspension from school, or school expulsion; or disciplinary actions to stall, including termination.

The information network services provided by New Plymouth may not always meet student or staff requirements or be uninterrupted or error-free. It is provided on an "as is, as available" basis. No warranties are made or given with respect to any service or any information or software contained therein.

VANDALISM

Vandalism will result in disciplinary actions. Vandalism is defined as:

1. Any attempt to harm or destroy data of another user, the district information network service, or other information network services. This includes, but is not limited to, the uploading or creation of computer viruses.
2. Any attempt to damage or modify any part of the computer system or hardware, specifically including mice, keyboards, speakers, disk drives, monitors, and printers.
3. Any attempt to impair the operation of the system or any of its components, including modifying the desk top, introducing viruses, or consuming more than authorized quantities of disk space or CPU time.

STUDENT DISCIPLINE

Violation of this policy may result in the following disciplinary actions:

1. First offense: The student will lose computer privileges and information network service access until a parent conference is held and disciplinary action determined.
2. Second offense: Any student who continues to engage in serious or persistent misbehavior by violating this policy may lose all computer privileges and information network service access for the remainder of the school year.
3. Students may be suspended or expelled from school if they engage in conduct on the information network service that could be considered unlawful or illegal, as defined by federal and/or state law. Students committing such acts may be prosecuted. Expulsion may be considered for flagrant violations of this policy.
4. **Each student is responsible for any damage he/she may cause to New Plymouth's computers or to the information network service. The student must pay all costs incurred in restoring the computer or the network service to its previous working order.**
5. If a class requires the use of a computer and/or the information network service, a student who has lost privileges under this policy may arrange to be allowed to participate with more limited access and under direct teacher supervision.

UPDATING USER ACCOUNT INFORMATION

A user's access to and use of the information network service may be terminated at anytime by the user or the user's parents or guardian by notifying a system administrator in writing.

An administrator has the right, at their sole discretion, to suspend or terminate a user's access to and use of the information network service upon any violation of this policy.

New Plymouth's administration, faculty, and staff may request the system administrator to deny, revoke, or suspend specific user account.