

COMPUTER NETWORK/INTERNET ACCEPTABLE USE

Island Trees Union Free School District

Introduction

The Island Trees school district has pursued making advanced technology and increased access to learning opportunities available to students. Our goal in providing these services is to meet the educational objectives of the district and to promote educational excellence by facilitating resource sharing, innovation, and communication in the global community.

The use of these computer resources throughout the district is a privilege. These resources include, but are not limited to, computer hardware, software, the Internet and online resources, peripherals, and communication devices. The district will provide teachers and students with access to the Internet that will enable users to explore thousands of libraries, databases, and web sites as part of the instructional process. Internet access from school computers will be supervised and reserved solely for educational purposes. It is the district's philosophy that having students identify, synthesize and use the vast, rapidly expanding electronic resources will build appropriate responsibility and techniques for sustainable lifelong learning.

The district will take precautions by using filtering software to help eliminate inappropriate Internet sites. The filtering policy (see policy 4526.1, Internet Safety) may not conform to the social values of every student or his/her family. By participating in the use of the Internet, students may gain access to information and communications which they or their parents/guardians may find offensive or inappropriate. The district cannot be held responsible for student access to these materials. Parents/guardians assume the risk by consenting to allow the students to participate in the use of the Internet. Students may use the Internet only if they have been granted parental permission and have submitted the required forms.

The smooth operation of the network relies upon the proper conduct of users who must adhere to strict guidelines. These guidelines are provided here so that users are aware of the responsibilities they are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. If a district user violates any of these provisions, his or her account may be restricted, suspended, or cancelled.

The signatures on the appropriate exhibit to this policy shall indicate that the parties who signed have read the terms and conditions carefully and understand their significance.

Acceptable Use Guidelines

The following guidelines have been established for acceptable use of the Island Trees School District's computer network and Internet access. Users must be aware that the district reserves the right to ensure compliance through electronic monitoring of network and Internet usage. Every effort will be made to maintain privacy and security in this process.

General:

1. The use of each account must be in support of education and research and consistent with the education objectives of the Island Trees School District. This means students are seeking information directly related to course and class work in the school. The district reserves the right to prioritize use and access to the system. Game sites, E-mail, auction sites (such as ebay), chat rooms, event booking, etc. cannot be accessed. Illegal activities are strictly forbidden and will result in disciplinary action.
2. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their passwords with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
3. Any use of the system must be in conformity to state and federal law, network provider policies and licenses and district policy. Use of the system for commercial solicitation is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent or designee.
4. The system constitutes public facilities and may not be used to support or oppose political candidates of ballot measures.
5. No use of the system shall serve to disrupt the operation of the system by others; system components including software and hardware shall not be destroyed, modified or abused in any way. Personal software or hardware may not be used on the system without permission. Food and beverages may not be brought into computer rooms or the school media center.
6. Malicious use of the system to develop programs that harass others or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.
7. Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, discriminatory or threatening remarks, or other antisocial behavior are expressly prohibited.
8. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.
9. The Superintendent or designee must approve subscriptions to mailing lists, bulletin boards, chat groups and commercial online services and other information services.

10. The use of the district network is a privilege to be used responsibly, fairly, and appropriately. The same behavioral expectations of students in school and the community apply to online behavior.
11. The rights of others to use the network without disruption must be respected at all times.
12. District-owned hardware and software must be treated with care to ensure its availability to others and should not be vandalized, damaged, stolen, or abused in any way.
13. The district cannot be held responsible for damages including loss of data resulting from delays or service interruptions. The district is not responsible for the accuracy or quality of information found on the Internet.
14. Downloading of files by students is limited to files related to instructional resources associated with school curriculum.
15. Users may not publish new web pages or modify existing web pages without the written authorization of a designated staff member.
16. Users may not download or upload files without authorization of a designated staff member.
17. Attempts must not be made to run or install programs that are not authorized by a designated staff member.
18. Attempts must not be made to intentionally degrade or disrupt the computer network, including the deliberate spreading of computer viruses.

Personal Security:

19. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their passwords with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
20. Users shall not seek information on, obtain copies of, modify files, other data or passwords belonging to others, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.
21. Communications may not be encrypted as to avoid security review.
22. Security guidelines will be developed and posted to address the frequency of password changes.
23. Communications and files on the district server are not private. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly.
24. Personal information such as names, addresses and telephone numbers must remain confidential when communicating on the system. Students must never reveal the personal information of themselves or others.
25. Students must never make contact with any person that they have contacted on the Internet.
26. Students must notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate or make them feel uncomfortable.

Ethical and Legal Considerations:

27. The use of the computer network must conform to district policies and local, state, and federal laws.
28. Use of the network to access, store, distribute or promote illegal activities such as bomb-making, drugs, gambling or pornography is prohibited.
29. Use of the network to promote racism, sexism, or other forms of discrimination is prohibited.
30. Use of the network to install, use, store, duplicate or distribute copyrighted materials, including software, files, video clips, photographs, text, music, or speech is prohibited.
31. Use of the network to plagiarize the work of others is prohibited.
32. Use of the network for non-school related promotion of political candidates or causes is prohibited.
33. Use of the network for commercial advertisements or profit-making purposes is prohibited.
34. Users must refrain from activities that may result in the district incurring any charges of damages.

Staff Responsibilities:

- A. It is the responsibility of staff members to help implement this policy by taking the following steps with their students:
 1. Inform all students through postings, orientations and reminders about the guidelines and behavioral expectations of students who have permission from a parent/guardian, including the consequences for misuse.
 2. Take reasonable measures to prevent students without parent/guardian permission from using the computer network.
 3. Take appropriate disciplinary actions when students violate any aspect of this policy.
 4. Report serious violations to an administrator.
 5. Respond immediately to student notification of dangerous, illegal, obscene, or inappropriate information transmitted over the computer network and report it to an administrator.
 6. Make sure that all computer monitors be clearly visible to the supervising teacher.
 7. Monitor and supervise content that users reproduce, exchange, or transmit through electronic means.
 8. Prohibit the use of any personal information electronically. This includes full name, home telephone numbers and addresses as well as information regarding the specific location of any student at any given time.

2. Notification of school authorities.
3. Notification of parent/guardian.
4. Permanent suspension of access to the computer network and the Internet.
5. Financial restitution.
6. Legal action including, but not limited to, criminal prosecution under appropriate state and federal laws.

Island Trees Union Free School District network facilities are to be used in a responsible, efficient, ethical, and legal manner in accordance with the mission of the district. Users must acknowledge in writing (see the attached forms) their understanding of the general policy and guidelines as a condition for using the networks.

Cross-ref: 4526.1, Internet Safety

Adoption date: February 27, 2008

Amended date: November 18, 2009

B. E-Mail Acceptable Use Guidelines:

“Acceptable” e-mail activities are those that conform to the purpose, goals, and mission of the Island Trees School District and to each user’s job duties and responsibilities. Users shall have no right to privacy while using the Island Trees internet or e-mail system. E-mail may not be used for personal purposes. “Unacceptable” use is defined generally as activities using Island Trees UFSD hardware, software, or network(s) at any time that does not conform to the purpose, goals, and mission of the district and to each user’s job duties and responsibilities. The following list, although not inclusive, provides some examples of uses:

1. Opening unknown e-mail attachments or introducing computer worms or viruses. Users are prohibited from performing any activity that will or may cause the loss or corruption of data or the abnormal use of computing resources (degradation of system/network performance).
2. Using e-mail services for private, commercial or business transactions and any activity meant to foster personal gain.
3. Using your e-mail address to subscribe to websites or other internet services that do not conform to your duties and responsibilities.
4. Conducting non-Department of Education fund raising or public relations activities such as solicitation for religious and political causes or not-for-profit activities
5. Transmitting threatening, offensive, or harassing information (messages or images) containing defamatory, abusive, obscene, pornographic, sexually oriented, racially offensive, or otherwise biased, discriminatory, or illegal data.

C. Teacher Web Pages Acceptable Use Guidelines:

Subject to district-wide policies and procedures, teachers may establish web pages for use with class activities or to provide a resource for other teachers and students. Teachers will be responsible for maintaining their class or educational resource sites. Teacher web pages will not be considered official material, but will be developed in such a manner as to reflect well upon the Island Trees UFSD. The Island Trees UFSD reserves the right to remove any teacher access to School World account should the site be misused or not keep current during the school year.

Consequences of Violations: The consequences for violating this policy may include **any one** of the following as determined by the Superintendent or his/her designee:

1. Restricted network access (i.e., temporary suspension or access to the computer network and the Internet.

COMPUTER NETWORK/INTERNET ACCEPTABLE USE SUMMARY**Island Trees Union Free School District**

The district has pursued making advanced technology and increased access to learning opportunities available to students and staff.

Our Goals are:

- To provide technology services which meet the educational objectives of the district.
- To promote educational excellence by facilitating resource sharing, innovation, and communication in the global community.

Our Resources include, but are not limited to:

- Computer hardware
- Software
- The Internet and online resources,
- Peripherals
- Communication devices

The use of these computer resources throughout the district is a privilege. The following guidelines have been established for acceptable use of the district's computer network and Internet access:

1. The use of each account must be in support of education and research and consistent with the educational objectives of the district.
2. System accounts are to be used only by the authorized owner of the account for the authorized purpose.
3. Any use of the system must be in conformity to state and federal law, network provider policies and licenses and district policy.
4. District-owned hardware and software should be treated with care to ensure its availability to others and should not be vandalized, damaged, stolen, or abused in any way.
5. Personal software may not be used on the system and downloading of files by students is limited to files related to instructional resources associated with school curriculum.
6. Food and beverages may not be brought into computer rooms or the school media center.
7. Users are responsible for the appropriateness and content of material they transmit or publish on the system.
8. The Superintendent or designee must approve subscriptions to mailing lists, bulletin boards, chat groups and commercial on-line services and other information services.

9. The district cannot be held responsible for damages including loss of data resulting from delays or service interruptions. The district is not responsible for the accuracy or quality of information found on the Internet.

Adoption date: February 27, 2008

COMPUTER NETWORK/INTERNET ACCEPTABLE USE EXHIBIT

Island Trees Union Free School District Internet Acceptable Use Authorization (Grades K-4) Parent/Guardian Permission Form:

Due to the content of the Acceptable Use Policy, younger children may not fully understand what is being conveyed; therefore, we recommend that you read and discuss the following with your child.

The Internet is a special tool that can help me learn, communicate and solve problems. Before I can use the Internet at my school, there are some promises I need to make to my teacher, my classmates, my parents and myself. These promises are made to keep me safe and to make my time on the Internet fun, interesting and educational.

- **I will** take care of the computer hardware and software so that it is available to others.
- **I will** be polite and courteous when online and use language that is respectful of others.
- **I will** never share personal information online including my name, address, phone number or picture.
- **I will** immediately tell an adult if I am asked anything that makes me uncomfortable or see anything that I don't understand.
- **I realize** that if I do not follow these guidelines, the privilege of using the district network and Internet will be suspended.

As parent/guardian of _____, I have read the "Internet Acceptable Use Policy" and understand the educational services that are available, the precautions that have been taken by the district to eliminate controversial material and the behavioral expectations and consequences that are in place. I have discussed these guidelines with my child and understand that my child's teacher will review this policy with my child as well.

By checking the appropriate box below, I give permission to my child to use the Internet through grades K, 1 2, 3 and 4. I have the right to withdraw my permission at any time. In order to do so, I will submit a written letter to the school principal.

I give my child permission to use the Internet.

I do not give my child permission to use the Internet.

Parent/Guardian Name: _____ **Phone:** _____
Signature: _____ **Date:** _____
School: _____ **Teacher** _____ **Grade:** _____

Disclaimer: Although the district has taken reasonable precautions, we cannot guarantee nor can we be responsible for the security, accuracy or appropriateness of content distributed through our network. The district will not be liable for financial or legal obligations arising from the unauthorized use of our system.

Adoption date: February 27, 2008

COMPUTER NETWORK/INTERNET ACCEPTABLE USE EXHIBIT

Island Trees Union Free School District
 Internet Acceptable Use Authorization (Grades 5-12)
 Parent/Guardian Permission Form:

As parent/guardian of _____, I have read the "Internet Acceptable Use Policy" and understand the educational services that are available, the precautions that have been taken by the district to eliminate controversial material and the behavioral expectations and consequences that are in place. I have discussed these guidelines with my child and understand that my child's teacher has already reviewed this policy with my child as well.

By checking the appropriate box below, I give permission to my child to use the Internet through grades 5, 6, 7, 8, 9, 10, 11 & 12. I have the right to withdraw my permission at any time. In order to do so, I will submit a written letter to the school principal.

I give my child permission to use the Internet.

I do not give my child permission to use the Internet.

Parent/Guardian Name: _____ Phone: _____

Signature: _____ Date: _____

If parent/guardian grants permission, please complete the following:

Student Contract:

I understand that when I am using the Internet or any other telecommunication environment, I must adhere to all rules of courtesy, etiquette and laws regarding access and copying of information as prescribed by either Federal, State or local laws, and the Island Trees Union Free School District. I have read the "Internet Acceptable Use Policy" and have discussed it with my parent/guardian.

My signature below, and that of my parent/guardian, means that I agree to follow the guidelines and will use the system appropriately at all times.

Student Name _____ Grade _____ School _____

Student Signature _____ Date _____

Disclaimer: Although the district has taken reasonable precautions, we cannot guarantee nor can we be responsible for the security, accuracy or appropriateness of content distributed through our network. The district will not be liable for financial or legal obligations arising from the unauthorized use of our system.

Adoption date: February 27, 2008

**COMPUTER NETWORK FOR EDUCATION EXHIBIT
ACKNOWLEDGMENT OR RESPONSIBILITIES**

I. EMPLOYER USER – INTERNET USER AGREEMENT:

This Agreement must be renewed each academic year.

I understand and will abide by the terms and conditions contained in the Island Trees Union Free School District's *Computer Resources and Data Management Regulation* No. 8630, and *Computer Network/Internet Acceptable Use Policy* No. 4526 and corresponding Regulations, copies of which I have received and read.

I acknowledge I have been advised I have no reasonable expectation of privacy when using District computers, networks, or internet, and that the District reserves the right to monitor such usage as it deems appropriate in order to protect the District and ensure compliance with District policies.

I understand that any violation of this Policy and/or Regulation may result in my access to privileges being revoked and/or the District taking disciplinary action and/or appropriate legal action against me.

In consideration for the privilege of using the District's Computer Network and in consideration for having access to the Internet, I hereby release the District, its Board of Education, employees, operators, and any institutions with which it is affiliated from any and all claims or damages of any nature arising from my use of, or inability to use, the Computer Network including, without limitation, the type of damages identified in the District's Policy and Regulation.

Employee's Name (Please Print)

Signature

Date

Adoption date: November 18, 2009
Amended date: October 27, 2010

INTERNET SAFETY

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The computer network coordinator designated under the district's Computer Network or Acceptable Use Policy, shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

Ref: Public Law No. 106-554
47 USC §254
20 USC §6801

Adoption date: February 27, 2008

INTERNET SAFETY REGULATION

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet and World Wide Web.

I. Definitions

In accordance with the Children's Internet Protection Act,

- Child pornography refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner than conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
- Harmful to minors means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.
- The district's computer network coordinator shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.
- The computer network coordinator or his or her designee may disable or relax the district's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.

- The computer network coordinator shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The district's computer network coordinator shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.
- Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's computer network coordinator shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

IV. Training

- The district's computer network coordinator shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web are directly related to their course work.
- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.

- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. Reporting of Violations

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.

Adoption date: February 27, 2008