

DIOCESE OF BRIDGEPORT, CONNECTICUT

ACCEPTABLE USE POLICY

2009-2010

Internet Safety and Computer Equipment Use Including Related Systems, Software, and Networks

By Students and Staff

I. Office for Education Responsibilities/Rights

1. To create an *Acceptable Use Policy* for the schools of the Diocese of Bridgeport
2. To publish said policy
3. To review it annually
4. To be free from liability for presence of unacceptable materials
5. To comply with State and Federal Regulations
6. To cooperate with authorities in criminal investigations
7. To be free from liability for financial obligation incurred through unauthorized use of system
8. To amend the policy at any time

II. School Responsibilities/Rights

1. To oversee resources including scheduling
2. To place reasonable restrictions on systems and technology
3. To perform routine system maintenance
4. To search individual Internet activity with reasonable suspicion
5. To own all files on school network
6. To be free from liability for presence of unacceptable materials on the school's system
7. To comply with Diocesan, State, Federal regulations
8. To provide a filtering system in accordance with CIPA, as protection measures
9. To provide opportunities for technological training for staff
10. To cooperate with authorities in investigations of criminal activities
11. To bypass passwords to determine activity
12. To publish student works on its website
13. To deny student/staff access

III. Parents'/Guardians' Responsibilities/Rights

1. To see their child's e-mail file upon request
2. To deny their children Internet access
3. To prevent the use of their children's names and pictures on the Internet by the school

IV. Student Privileges/Expectations/Understandings

1. To use Internet in distance learning
2. To access World Wide Web for educational purposes
3. To have individual e-mail accounts to send and receive e-mail
4. To receive instruction in technology use
5. To have reasonable protection measures
6. E-mail or Internet correspondence is not privileged or confidential
7. To use Internet to consult experts
8. To communicate with other students
9. To locate information to meet educational needs
10. To have staff assistance to find, use, discriminate among, information sources

V. Prohibitions

1. Modifying documents or files without permission
2. Playing unauthorized games
3. Making purchases
4. Conducting commercial or private business
5. Personal use – unrelated to appropriate educational purposes
6. Political lobbying
7. Installing software for personal use
8. Installing school software at home without school permission
9. Altering, interfering with, dismantling, disengaging Internet
10. Installing educational software without Office for Education permission
11. Installing stand alone (CD/Diskette) without Office for Education approval
12. Illegal activities
13. Accessing knowingly inappropriate material
14. Downloading large files without permission
15. Sending chain letters
16. Spamming
17. Plagiarizing
18. Copyright infringements
19. Profane, obscene language/defamation
20. Accessing and transmitting pornography
21. Accessing information advocating violence or discrimination outside the scope of research under direction of a teacher/supervisor
22. Accessing, modifying, erasing, rename, making usable or unusable another's files or programs
23. Modifying, copying, transferring software provided by school, faculty, another student without permission
24. Aiding or abetting another student in policy violation
25. Introducing or spreading viruses or other harmful programs
26. Divulging passwords

VI. Individual Responsibilities

1. To comply with security measures
2. To report illegal activities
3. To report improper language or unacceptable activities on the Internet
4. To report damage or tampering with equipment or system
5. To report violations of privacy

VII. E-Mail Etiquette

1. Be patient
2. Be polite
3. Keep paragraphs short
4. Use "Subject Line"
5. Include signature
6. Capitalize only to highlight important points