INTERNET SAFETY POLICY

It is the policy of RAILS to:

a) Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, email, or other forms of direct electronic communications;

b) Prevent unauthorized access and other unlawful online activity;

c) Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

d) Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions

Key terms are as defined in the Children's Internet Protection Act.

Access to Inappropriate Material

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Technology protection measures may be disabled for adults for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the RAILS online computer network when using email, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

a) Unauthorized access, including so-called 'hacking,' and other unlawful activities; and

b) Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

RAILS computers are intended for use by staff working at RAILS facilities or remotely. Some computers are also designated for use by adults attending workshops or meetings at RAILS facilities. Use of RAILS computers by persons under the age of 18 is prohibited except under the direct supervision of a RAILS staff member.

Education, Supervision and Monitoring

It shall be the responsibility of all members of the RAILS staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act. Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of the Director of Technology Services or designated representatives.

Commented [AS1]: Is the intended scope of this policy limited to the requirements of CIPA? We don't have a more generalized cyber security policy, though security is addressed in remote work and equipment use policies. Are we missing anything that should be addressed in policy?

Commented [AS2]: From Wes: We no longer file for erate, we are no longer required to follow CIPA. I think some of the requirements are justified and should be part of the policy but at the time this was written we were required to abide by the CIPA guidelines to secure erate funding.

Commented [AS3R2]: If there's no longer a need to maintain this policy specifically, in the absence of the erate requirement, maybe anything that isn't already covered in the equipment use policy can be incorporated there? The language of that policy already encompasses internet use (communication services, transmission of information, etc.)

Commented [AS4]: From Wes: This can cause problems with staff needing to access material such as art, that software deems inappropriate. I suggest we do away with the content filtering as we are not publicly accessible and no longer bound by CIPA. I think that dealing with employee behavior is a better route than blanket blocking website access based on software. Policy about viewing sexually explicit material and not breaking laws should be enough.

Commented [AS5]: What is the expectation/purpose of this statement? IT monitors the network and provides training. Is "comply with" enough?

Commented [AS6R5]: From Wes: So vague and staff is not trained to educate, supervise and monitor appropriate usage of the "Online Computer Network"

Commented [AS7]: From Wes: More CIPA language that is not necessary. Clear guidance would be:

1) Do not engage in illegal activity on RAILS equipment and if you see it happening you should report it.

2) Do not engage in activities that would be inappropriate for a work environment. Such has playing games or viewing sexually explicit material and if you see it happening you should report it.