Arkansas Department of Human Services
DYS Minor Internet Protection Policy
(DRAFT)

Attachment W

I. Policy

The Arkansas Department of Human Services Division of Youth Services any authorized providers/vendors/suppliers shall prevent student access to or transmission of inappropriate content via the internet, email or other forms of electronic communication; prevent authorized access to the internet by students; and prevent unauthorized online disclosure, use or dissemination of personal identification information of students.

Juvenile Justice clients shall use the internet only in educational or instructional programs.

II. Standards

A. Youth are prohibited from access to or use of computers and other electronic devices others than those designated for student use. Youth will not use computer established for staff use, unless under one-on-one supervision for extenuating circumstances.

B. Youth will have access to specific educational websites during school hours, as designated by the Division of Youth Services. Youth are prohibited from access to public email services, chat rooms, instant messaging, social networking and other forms of direct electronic communication.

C. Youth will adhere to the DYS Student Computer Use and Internet Safety Policy [Policy Number]

D. Education programs, post secondary applications, financial aid applications, and job searches may require students to obtain an e-mail address. In the event the student needs an e-mail, it must be created by the Arkansas Department of Human Services Office of Systems and Technology (OST) on an internally secure and monitored system.

E. DYS staff shall directly supervise and constantly monitor youth who are using the internet.

F. The use of computer and the internet is a privilege, not a right. There is no expectation of privacy. School administrators, with the approval of the Superintendent, may deny, revoke or suspend youth access at any time, with or without cause.

G. If DYS staff suspects a security breach, usage of the device or computer will be immediately suspended. DYS staff will immediately notify the facility Director and complete a special incident report. Education staff will notify the Superintendent and

secure the device or computer in a locked location until it is determined if an investigation is warranted. Education staff will also submit a request to the help desk to notify the Office of the CISO.

H. Youth will be instructed to immediately notify staff if a security breach has occurred. Education staff will investigate to determine if further measures should be taken.

III. Technology Protection Measures

A. DYS will use technology protection measures, to the extent possible, to block the access of inappropriate content via the internet or other forms of electronic communication.

B. The list of authorized education websites that youth can access can only be modified upon request of the Superintendent to the Chief Information Officer (CIO) or Chief Information Security Officer (CISO) of the Office of Systems and Technology. All requested websites must be tested to determine whether any inappropriate websites can be accessed by links.

C. Education staff must maintain technology protections measures at all times. The Office of Systems and Technology will ensure the certification of youth internet protection to the Federal Communications Commission.