GEORGIA DEPARTMENT OF JUVENILE JUSTICE	Transmittal # 18-16	Policy # 13.13
Applicability: { } All DJJ Staff {x} Administration { } Community Services {x} Secure Facilities	Related Standards & References: Children's Internet Protection Act §47 USC 254(h) and (i) 47 CFR 54.520 ACA Standards: 3-JDF-5C-03, 4-JCF-5D-02, 3-JDC-5C-04-4 DJJ 6.2, 8.5	
Chapter 13: EDUCATION	Effective Date: 8/31/18 Scheduled Review Date: 8/31/19 Replaces: 8/31/17 Office of Education APPROVED: _____ Avery D. Niles, Commissioner	
Subject: YOUTH INTERNET USE AND SAFETY		
Attachments: None		

I. POLICY:

In accordance with the Children's Internet Protection Act, the Department of Juvenile Justice shall prevent student access to or transmission of inappropriate content via the internet, email, or other forms of electronic communication; prevent unauthorized access to the internet by students; prevent unlawful online activity by students; and prevent unauthorized online disclosure, use, or dissemination of personal identification information of students. Department of Juvenile Justice-Georgia Preparatory Academy (DJJ-GPA) students shall use the internet only during instructional programs.

II. DEFINITIONS:

Security Breach: Student's access of unauthorized websites or any use of e-mail, instant messaging, social networking, or other forms of direct electronic communication.

Technology Protection Measure: A specific technology that blocks or filters internet access to visual depictions that are obscene, child pornography, material harmful to minors, sexual acts, or sexual contacts as defined in the Children's Internet Protection Act.

III. PROCEDURES:

A. Youth are prohibited from access to or use of computers and other electronic devices other than those designated for student use. Youth will not use computers established for staff use, unless under one-on-one supervision for testing, postsecondary options, career advisement, and student surveys.

B. Youth will have access to specific educational websites during school hours, as designated by the Office of Education. Youth are prohibited from access to chat rooms, instant messaging, social networking, or other forms of direct electronic communication, with the exception of required communication for post-secondary options.

C. Education programs, postsecondary 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 an education staff member with the school leader's approval. The staff member will maintain the security of the email account until release.

D. DJJ staff shall directly supervise and constantly monitor youth who are using the internet.

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

F. If DJJ staff suspect a security breach, usage of the suspected device or computer will be immediately suspended by removing the power cord. DJJ staff will immediately notify the facility Director and follow in-house Special Incident Report (SIR) procedures in accordance with DJJ 8.5, Special Incident Reporting. Education staff will notify the Regional Principal and Education Technology Manager.

G. Youth will be instructed to immediately notify staff if a security breach has occurred. Education staff will immediately notify the Education Technology Manager and the Office of Technology and Information Services in accordance with DJJ 6.2, Network Access. Staff must also complete an in-house Special Incident Report.

IV. TECHNOLOGY PROTECTION MEASURES:

A. DJJ 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 educational websites that youth can access can only be modified upon request of the Associate School Superintendent to the Director of the Office of Technology and Information Services. All requested websites must be tested to determine whether any inappropriate websites can be accessed via links.

C. Computers designated for youth access must be maintained on a separate network from other DJJ users.

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

V. LOCAL OPERATING PROCEDURES REQUIRED: NO