

<p align="center">GEORGIA DEPARTMENT OF JUVENILE JUSTICE</p>	<p align="center">Transmittal # 16-3</p>	<p align="center">Policy # 13.13</p>
<p>Applicability: <input type="checkbox"/> All DJJ Staff <input checked="" type="checkbox"/> Administration <input type="checkbox"/> Community Services <input checked="" type="checkbox"/> Secure Facilities (RYDCs and YDCs)</p>	<p>Related Standards & References: Children’s Internet Protection Act (47 USC 254(h) and (i) 47 CFR 54.520 3-JDF-5C-03, 4-JCF-5D-02, 3-JDC-5C-04-4</p>	
<p>Chapter 13: EDUCATION</p>	<p>Effective Date: 2/9/16 Scheduled Review Date: 2/9/17</p>	
<p>Subject: YOUTH INTERNET USE AND SAFETY</p>	<p>Replaces: 10/20/14 Education and Re-Entry Services</p>	
<p>Attachments: None.</p>	<p>APPROVED:  _____ Avery D. Niles, Commissioner</p>	

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 students shall use the internet only in instructional programs.

II. DEFINITIONS:

GeorgiaCollege411.org/GAfutures.org: A website that helps students plan, apply, and pay for college. It is a free service of the State of Georgia provided by Georgia Student Finance Commission (GSFC).

Security Breach: Student 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

Chapter	Subject	Policy #	Page
EDUCATION	YOUTH INTERNET USE AND SAFETY	13.13	2 of 3

for staff use, unless under one-on-one supervision for extenuating circumstances, i.e. testing and/or postsecondary options.

- 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.
- 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 through GA College 411(GAfutures.org).
- 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, with the approval of the Associate School Superintendent, may deny, revoke, or suspend youth access at any time, with or without cause.
- F. If DJJ staff suspects a security breach, usage of the device or computer will be immediately suspended. DJJ staff will immediately notify the facility Director and complete an In-house Special Incident Report (SIR). Education staff will notify the Regional Principal and secure the device or computer in a locked location until it is determined if an investigation is warranted.
- G. 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.

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 Chief Information Officer (CIO) 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. The Office of Education will designate staff to monitor approved websites on a monthly basis and/or as updates occur to determine if the website has been changed to include additional links.
- D. Computers designated for youth access must be maintained on a separate network from other DJJ users.

Chapter	Subject	Policy #	Page
EDUCATION	YOUTH INTERNET USE AND SAFETY	13.13	3 of 3

- E. 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