BUILDING THE TECHNOLOGY ECOSYSTEM FOR CORRECTIONAL EDUCATION:

BRIEF AND DISCUSSION GUIDE

August 2022

This page is left intentionally blank.

Building the Technology Ecosystem for Correctional Education:

Brief and Discussion Guide

August 2022

U.S. Department of Education
Miguel A. Cardona, Ed.D
Secretary

Office of Career, Technical, and Adult Education
Amy Loyd, Ed.L.D.
Assistant Secretary

This document is available on the Department's website at https://lincs.ed.gov/sites/default/files/tech-ecosystem-correctional-ed.pdf

Availability of Alternate Formats
On request, this document is available in alternate formats, such as braille, large print, or audiotape. For more information, please contact the Department's Alternate Format Center at 202-260-0852 or by emailing alternateformatcenter@ed.gov.

Notice to Limited English Proficient Persons
If you have difficulty understanding English, you may request language assistance services for Department information that is available to the public. These language assistance services are available free of charge. If you need more information about interpretation or translation services, please call 1-800-USA-LEARN (1-800-872-5327) (TTY: 1-800-437-0833), or email us at Ed.Language. Assistance@ed.gov. Or write to U.S. Department of Education, Information Resource Center, LBJ Education Building, 400 Maryland Ave. SW, Washington, DC 20202.

All URLs were accessed on the dates indicated. If a URL is not valid, it's because the publisher removed the material or changed its location.

Content Contact:
Sean Addie
Phone: 202-245-7374
Email: Sean.Addie@ed.gov

CONTENTS

EXHIBITS

ABBREVIATIONS

CDOC	Colorado Department of Corrections
CTE	career and technical education
DOC	department of corrections
FAFSA®	Free Application for Federal Student Aid®
FEDRAMP	Federal Risk and Authorization Management Program
FERPA	*Family Educational Rights and Privacy Act*
IT	information technology
LAN	local area network
LDPSC	Louisiana Department of Public Safety and Corrections
LMS	learning management system
MATC	Milwaukee Area Technical College
MDOC	Maine Department of Corrections
ODRC	Ohio Department of Rehabilitation and Corrections
SOP	standard operating procedure
WAN	wide area network
WDOC	Wisconsin Department of Corrections

ACKNOWLEDGMENTS

FOREWORD

Dear Corrections Administrators and Educators:

The Office of Career, Technical, and Adult Education at the U.S. Department of Education is pleased to share this brief and discussion guide to help states develop and sustain the necessary policy, programmatic, and technical environments to expand the use of technology in correctional education. We believe that safely and effectively using technology to support high-quality instructional strategies is critical to preparing individuals for success after their release and for increasing digital equity nationwide.

The Office of Educational Technology describes the conditions for achieving digital equity in education as requiring a careful balance and integration of the various aspects of technology-enabled learning environments. These aspects include
- an information technology (IT) infrastructure that provides students with reliable access to content, leverages appropriate security protocols, and maintains clear expectations for protecting student privacy;

- supports for students to help them gain the skills necessary to successfully navigate a technology-enabled environment, such as information and data literacy; and

- educators trained in effective uses of technology, which include expanding the resources that are available to students, personalizing instruction with those resources, and guiding students as they build, create, and improve content using technology.

This brief primarily focuses on the first aspect, building an IT infrastructure for correctional education, as an important foundation for offering quality technology-enhanced teaching and learning experiences in correctional education. We believe, however, that the foundation should be aligned with a vision for how technology-enabled instruction will mirror successful uses of educational technology by programs in the community, especially to support students continuing their education after release from incarceration.

In working with our colleagues at the U.S. Department of Justice and other federal agencies, as well as other partners across the country, we recognize and appreciate the role that corrections administrators and educators play in supporting digital equity within correctional systems. They are increasingly finding secure methods to provide students with access to technology to support learning. As access and use increase, more research is needed to understand how different technologies impact student outcomes and to identify effective instructional strategies within the corrections context. We are encouraged, however, by the examples shared in this brief of how states are expanding access to educational technology in corrections and increasing digital equity and hope that it inspires you to participate in this important work.

Sincerely,
Amy Loyd, Office of Career, Technical, and Adult Education
Kristina Ishmael, Office of Educational Technology

INTRODUCTION

The *Educational Technology in Corrections 2015* brief described efforts to provide secure and cost-effective access to technology in correctional facilities to help strengthen and expand educational and reentry services (U.S. Department of Education 2015). Since then, much has changed about how we access and use technology in everyday life, including education. The same is true for corrections. In recent years, correctional education leaders have begun to expand the use of technology across education levels, with a focus on securely using technology to improve students' educational experiences and skills.

Some of this expansion occurred in response to the COVID-19 pandemic inside U.S. prisons and jails. As in-person education was cancelled, education and corrections leaders explored technology solutions to deliver education to incarcerated students safely and at a distance. These changes started as early as 2015, however, when the U.S. Department of Education announced a new experiment under the Secretary of Education's Experimental Sites Initiative authority to provide waivers to 67 colleges and universities of the prohibition on the use of Pell Grants by students in federal and state prisons (U.S. Department of Education 2015). This initiative encouraged many departments of corrections (DOCs) that partnered with the Second Chance Pell education institutions to revise their policies and begin to allow postsecondary programs offered inside correctional facilities to use the same or similar technology as those on the outside (see **Exhibit 1** for more details). The experiment has since been expanded to include more institutions of higher education, most recently in April 2022.

The expanded use of technology in correctional education is also driven by an increased focus on digital literacy as a key component of increasing digital equity. All students need to know how to skillfully navigate the different ways that technology intersects with society, particularly as it relates to participating in education programs, searching for and applying for jobs, performing work duties, communicating with family and friends, or accessing community and medical services. The *Workforce Innovation and Opportunity Act of 2014* (29 U.S.C. § 3101, *et seq.*), which provides funding for correctional education programs, supports technology integration to improve teaching and learning and recognizes digital literacy skills as a key component of workforce preparation activities for education and training programs. If students are not exposed to technology while incarcerated, they may face even greater challenges upon release.

For these reasons, it is no longer a question of "if," but "how," we integrate technology into correctional education programs. In corrections, however, the "how" is typically driven by security requirements, rather than instructional needs, and access to technology for educational purposes is still limited in many correctional institutions. Moreover, little research exists on the effectiveness of technology uses or best practices for integrating technology into instruction in correctional education. Expanded access to technology in corrections does not necessarily reflect technological progress in the community nor is it consistent across states or correctional institutions. For example, in many correctional facilities, students still may not have access to computers, let alone the internet, so technological expansion in some state correctional systems might involve the creation of a computer lab or adoption of offline web content. Only a few states have developed a comprehensive technology ecosystem for correctional education that involves one laptop or device per student, open internet access, and the use of videoconferencing, and of those that have, more research and evaluation is needed to understand the impact of technology use on student outcomes.

This update to *Educational Technology in Corrections 2015* is designed to help education and corrections leaders understand key issues in adopting and integrating technology to support instruction across adult education, career and technical education (CTE), and postsecondary education more broadly. It begins with a section describing the components of a state correctional education technology ecosystem, with a focus on the technical infrastructure and a summary of best practices for using educational technology in the community that can be applied to corrections. It then includes profiles of four state ecosystems (Colorado, Louisiana, Maine, and Wisconsin) and synthesizes lessons learned across these states. The final section, the Discussion Guide, provides a tool for guiding state-level conversations about the policy and technical components needed to develop a state correctional education technology ecosystem. Corrections and education leaders can use this resource to understand the technical and other components necessary to further expand the use of technology in correctional education programs.

ECOSYSTEM OVERVIEW

STATE PROFILES

DISCUSSION GUIDE

NEXT STEPS AND RECOMMENDATIONS

EXHIBIT 1. SECOND CHANCE PELL EXPERIMENT

The Second Chance Pell experiment, conducted under the Experimental Sites Initiative and launched by the U.S. Department of Education in 2015, provides need-based Pell Grants to people in state and federal prisons who otherwise would have been ineligible for Pell Grants. The initiative examines whether expanding access to financial aid increases incarcerated adults' participation in educational opportunities. In 2016, 67 colleges were selected to participate and in 2020, the initiative was expanded to include 130 colleges from 42 states and the District of Columbia. In the spring of 2022, the Department of Education announced that it was inviting an additional 73 programs to participate, providing up to a total of 200 institutions of higher education the ability to participate in the 2022–23 award year. Thus far since implementation, more than 25,000 students have participated in the experiment.

On behalf of incarcerated students, participating postsecondary education institutions use Pell Grants to pay for tuition, books, supplies, and fees. Fees include the cost of technologies (e.g., laptops, tablets, and software) used by some colleges to enhance in-person instruction or provide online instruction. The need for technology increased with the pandemic when departments of corrections severely restricted access to prisons to limit the spread of the virus and many Second Chance Pell colleges could no longer offer in-person instruction. Departments of corrections and colleges implemented emergency remote learning strategies and tools to continue providing education to students during pandemic lockdowns. Some of these tools include web conferencing, internet access, tablets and laptops with learning management systems, and heavy equipment simulators.

COMPONENTS OF A CORRECTIONAL EDUCATION TECHNOLOGY ECOSYSTEM

Safely and thoughtfully integrating educational technology into state correctional education systems begins with developing a vision for the intended instructional experience for students. How will students interact with the technology and with instructors? What strategies will instructors use to integrate technology into the classroom to enhance student learning and promote digital equity? This vision should drive all state decisions about technology integration, where possible, and requires an understanding of the technical components, instructional approaches, and other state supports needed to implement the vision. State leaders should first consider why technology will be used, along with what technology to use and how it will be used, to connect students both with educational content or platforms and with instructors for the delivery of educational content. The interplay of these components — the why, what, how, and who — of technology use make up a correctional education technology ecosystem (see **Exhibit 2**).

EXHIBIT 2. CORRECTIONAL EDUCATION TECHNOLOGY ECOSYSTEM COMPONENTS

WHY
Vision for technology integration

HOW
Instructional strategies

- Instructor-led synchronous learning
- Instructor-led asynchronous learning
- Self-directed learning
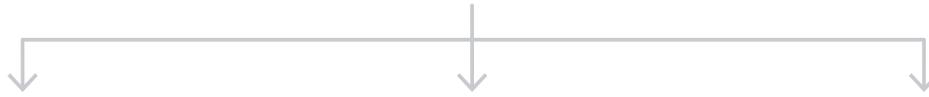
WHO
Student-centered ecosystem

- Program staff
- State agencies
- Students
- Instructors
- IT vendors
- Facilities staff

WHAT
IT Infrastructure

- Hardware
- Software
- Network access
- Physical infrastructure
- Data
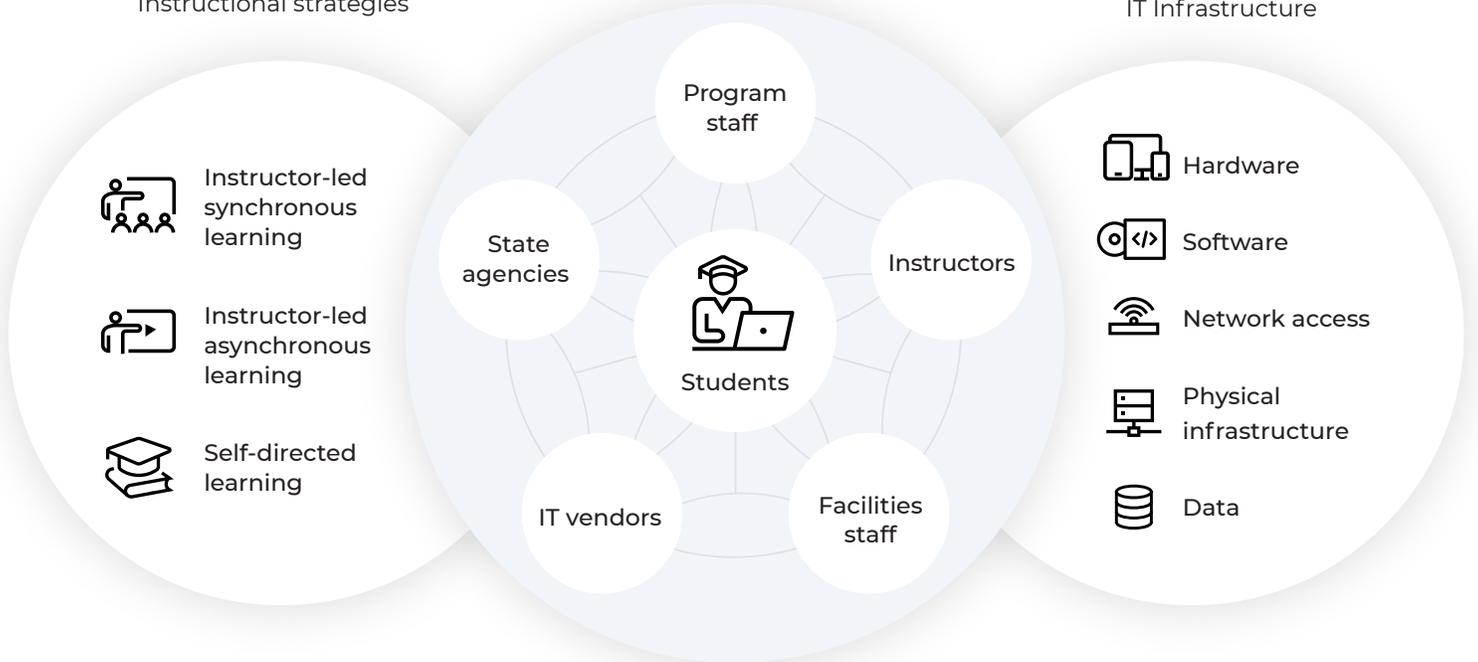
CONSIDERATIONS

Device selection/maintenance | Funding | Security | Staffing and teacher development

Student preparation | Teaching and learning | Vendor selection

This section describes the components of this ecosystem, with a summary of best practices for incorporating technology into teaching and a focus on building the necessary technical infrastructure to help corrections leaders meet the twin goals of quality programming and adequate security.

Technology-Supported Instructional Approaches

As noted in the introduction, the use of technology in correctional education brings added security considerations, which often results in the technical infrastructure driving decisions about technology needs and instructional strategies. Ideally, technology choices would be informed by instructional or learning goals, so that selected technology is used to enhance the instructional experience. As such, instructors using technology become the "guides, facilitators, and motivators of learners" according to the U.S. Department of Education's National Education Technology Plan (2017). Instructors can assume these roles by integrating technology in different ways and with varying amounts of support that range from self-directed student learning to instructor-led approaches (Vanek, Simpson, and Goumas 2020).

Although the current research base does not focus on corrections, it does highlight best practices for using educational technology in the community, especially with historically underserved students, that can be applied to correctional education. For example, Digital Promise (Constantakis 2016) offers a model for integrating technology in adult education that aligns with key principles of adult learning theory: experience based, centered on problem-solving, allows for reflection, enables self-directed learning, and supports transformative learning. Other best practices center on providing authentic learning experiences, encouraging collaboration (among peers and instructors), and extending learning beyond the classroom (Edutopia 2007; Rosen and Vanek 2020; U.S. Department of Education 2017). See **Exhibit 3** for a summary of research-based best practices for integrating technology into education programs.

EXHIBIT 3. SUMMARY OF INSTRUCTIONAL APPROACHES FOR USING TECHNOLOGY

Research and policy guidance highlight the following best practices for integrating educational technology into instruction (Darling-Hammond, Zielezinski, and Goldman 2014; Escueta et al. 2017; Reich and Ito 2017; U.S. Department of Education 2017). The practices span both the access to and use of technology, but they imply that just providing access to technology alone will not enhance student learning. Rather, personalized and interactive instructional strategies are needed to help students make the best use of technology.

- Ensure equitable access to technology especially for historically underserved students.
- Combine online and in-person instructional experiences (e.g., blended learning), rather than providing only online instruction.
- Use technology to allow students to apply problem-solving skills and explore and create content, rather than just to practice drills.
- Ensure technology provides interactive experiences for students and encourages them to collaborate with and learn from their peers.
- Provide ongoing support to teachers, including opportunities for professional learning on how to integrate technology into the classroom and standards for digital learning.

Instructional approaches should resemble those that are used in the community to provide technology-supported instruction, especially to ensure continuity between programs students may participate in while incarcerated and after release and to ensure digital equity and opportunity for students. This brief identifies three approaches for offering technology-supported instruction in correctional education. These approaches are adapted from a recent report from Ithaka S+R, which described three models for using instructional technology in correctional education for college programming (Tanaka and Cooper 2020).

Self-directed learning
Students access educational content on their own — often from a third-party vendor — and complete online programs or credentials without direct instruction from a correctional education provider. Students can work at their own pace within housing units. For example, many high school equivalency software packages use self-directed instruction. In this approach, students benefit from the support of a caring mentor who can facilitate communication between students and the instructional program and encourage student persistence and engagement[1].

Instructor-led synchronous learning (in person or online)
Students participate in live instructional activities in an online or partially online environment. This includes virtual "face-to-face" instruction in which an instructor conducts class using videoconferencing technology and digital tools, with classes meeting both in person and online at different times. Students use technology to attend virtual classes and access content or complete assignments. For example, an instructor broadcasts a scheduled lesson from one location to students who connect from their own devices at other locations.

Instructor-led asynchronous learning (in person or online)
Students participate in instructional activities on their own time, as assigned by instructors. Students use technology to communicate with instructors and to access content or complete assignments. This includes, for example, the use of computer labs to conduct research or the use of tablets to view reading material. For example, in a flipped-classroom model, students watch videos recorded by instructors or access assigned reading material on their own time and then use scheduled class time to ask questions, discuss assignments with instructors, and apply their learning.

---

[1] See https://michiganvirtual.org/blog/what-does-research-say-about-mentoring-online-students.

To date, no evaluation has been conducted of these approaches for correctional education, so they are presented as examples of instructional strategies that are commonly used. More information, as well as further research and evaluation, is needed to determine the quality of these approaches for correctional education and to analyze the outcomes of their use over time.

Technical Infrastructure

The technical requirements to support the use of educational technology in corrections include the **hardware**, or the tools and equipment needed to connect students with instructors and/or educational resources; **software** to provide content or manage a program; cybersecurity and **network access** to safely connect hardware and software; **physical infrastructure** to determine where students will use technology and the tools needed to maintain it; and **data** needed to measure student progress and track their technology usage.[2]

Hardware and Software for Educational Technology

Education providers in correctional facilities use many technologies commonly available to schools and colleges in the community, including laptops and desktops, learning management systems (LMSs), and videoconferencing tools. Adult education instructors and students use software packages like those found in high school equivalency classes outside of correctional facilities. However, while the technology is similar, it is often secured (e.g., hardened) to meet the security needs of the prison environment.

Common hardware and software used in correctional education includes the following:

Tablets, laptops, or desktops
These devices often have additional physical and software security for use in correctional facilities and vary in size from 5-inch tablets to 13-inch laptops to full desktops with multiple monitors depending on program need.

Curriculum and textbooks
Education providers purchase curriculum, instructional software, and e-textbooks to provide course materials for adult education and postsecondary education. They also may adopt or create open educational resources for these purposes.

---

[2] For further details on technology infrastructure for education in general, see the U.S. Department of Education's June 2017 report, *Building Technology Infrastructure for Learning*, available at https://tech.ed.gov/files/2017/07/2017-Infrastructure-Guide.pdf

Learning Management System (LMS)

A software application to organize and deliver course material, an LMS may be available via a live Internet connection, locally hosted on an education local area network (LAN), or installed on an individual device.

Library resources

In addition to web resources or catalogs available from libraries, vendors have developed locally hosted and web-based solutions for use in correctional education programs so that students can access indexes of articles, abstracts, and in some cases full-text materials.

Video or Web conferencing

Multiple vendors provide software applications for live video interaction and/or hardware, such as cameras.

Web resources

Several education providers host collections of web resources specifically for use offline. Many of these resources are open educational resources that can be hosted on a network or installed on a device.

Network Access, Cyber Security, and Infrastructure in Correctional Facilities

When providing network access in correctional facilities, security is paramount and involves considerations related to intentionally getting content into the facility through the internet and securing the network to keep out unwanted content. To do both, facilities need a well-designed and secure infrastructure maintained by licensed professionals.

Designing and Securing a Network

Network access is critical to using educational technology in correctional education programs. Students must be able to access online content and communicate with instructors and their peers, whether asynchronously or at a distance. At the same time, correctional facilities must ensure the security of network access, which often means preventing students from accessing any online content outside of their education program. To meet security requirements, therefore, correctional facilities tend to provide network and/or internet access for educational purposes in one of the following three ways (U.S. Department of Education 2015):

- Using an **isolated local server** to provide access to offline content that has been moved to a facility's LAN. While very secure, because students can only access approved content, this approach requires frequent uploading of internet content and does not provide real-time access to the internet.

- Operating a **point-to-point secure line** between the facility and an internet service provider to stream online content via a virtual circuit setup. This allows students to securely access the internet in real time, but it can be costly due to vendor fees.

- Providing limited content through a **restricted internet connection** that has routers and firewalls on each end. This allows students real-time access to essential software programs and applications and preapproved, or "whitelisted," content. It can be expensive because of monthly vendor fees.

Some states may contract with vendors to provide secure access to the internet and cybersecurity support. For example, vendors might provide internet access through a tablet or other device that only updates and syncs educational content when docked at a kiosk, typically located in a computer lab or classroom. A wide variety of vendors provide such network access, ranging from large telecommunications firms providing commercial internet to companies specializing in educational content for incarcerated individuals. Vendors also provide security support for correctional systems, such as by developing a "hack kit" for states to try to break or hack into the vendor's technology solution to demonstrate security procedures and gain buy-in from IT administrators about the trusted security of the network or device.

Developing Physical and Data Infrastructure

For the education hardware and software to be operationalized and allow for effective educational technology services to be delivered to students, correctional facilities must put in place a basic physical and data infrastructure. At a very high level, this includes the physical infrastructure needed to maintain internet access, the physical layout of the classroom, and security considerations for taking tablets or laptops back to the housing units. It also includes maintaining and securely storing hardware.

The infrastructure involves maintaining educational software and student data across multiple platforms like student information systems[3] or LMSs that can allow state agencies or correctional facilities to track student progress within specific education programs and can follow students as they transfer to different facilities or are released. States also must ensure the protection of student data in accordance with *Family Educational Rights and Privacy Act* (*FERPA*) (20 U.S.C. § 1232g), which is a federal law that, where applicable, among other things, generally prohibits *FERPA*-covered education agencies (e.g., school districts) and institutions (e.g., schools) from disclosing personally identifiable information from the education records of a student without the prior written consent of the student's parent or an eligible student, unless an exception to the general consent requirement applies. As states expand their use of educational technology for correctional education, policies and procedures should be developed to maintain the physical infrastructure and protect student-level data[4].

---

[3] A student information system collects data on student demographics, enrollment, scheduling, and progress.

[4] More information about *FERPA* is available from the U.S. Department of Education's Student Privacy Policy Office's website at https://studentprivacy.ed.gov.

Expanding Access

The Educational Technology in Corrections 2015 brief included profiles of state and local corrections agencies that were in the early stages of technology adoption. Since then, several sites have expanded use of technology for correctional education. Some examples include the following:

- **Leveraging new funding opportunities to expand technology use**
  In 2015, the Ohio Department of Rehabilitation and Corrections (ODRC) started using tablets that had locally installed educational content. Five years later in December 2020, ODRC had moved from static locally installed content to a student wireless network — a Wi-Fi network separate from the state's administrative network specifically for incarcerated students. ODRC purchased laptops with funds from the Coronavirus Aid, Relief, and Economic Security Act (2020) (H.R. 748, Public Law 116-136) to provide expanded access to educational content in classrooms and housing units for thousands of students. Students now can access preapproved online resources, including platforms that offer access to secondary courses, through a restricted internet connection and use laptops to complete asynchronous coursework under direct supervision of a teacher or other program staff or contractor.

- **Designing instructional strategies to support statewide expansion**
  Based on the success of one college's development of an isolated local server to provide access to educational content within correctional facilities, eight community colleges in Washington now provide offline laptops with a self-hosted learning management system (LMS) for use within all state department of corrections facilities. The fully offline laptops sync with the LMS and can be used in the housing units. State education leaders developed a repository of openly licensed instructional materials — resources that are freely available and can be adapted by users — to support a flipped-classroom approach. Instructors deliver content through the LMS, students read the material and complete assignments in their housing units, and classes meet on a predetermined schedule to discuss the content, answer questions, and take quizzes and exams.

- **Embracing holistic approaches to technology integration**
  The Multnomah Education Service District, in partnership with the Oregon Youth Authority, integrates technology into all education services to eight youth corrections schools and programs. For example, students can use heavy equipment simulators in career and technical education classes, such as working in fabrication labs and using a driving simulator. Programs also integrate technology into more creative courses, such as by offering creative suite tools for workshops and art classes using tablets and pens.

STATE ECOSYSTEM EXAMPLES

The following profiles, developed through interviews with state corrections leaders, describe the state context, strategies, and supports for using educational technology in Colorado, Louisiana, Maine, and Wisconsin, all states that have expanded technology use over the past five years. While some of these examples reflect responses to the COVID-19 pandemic, as many states shifted to distance learning approaches so that education programming could continue in correctional institutions, they all started with (and maintained, to the extent possible) in-person instructional components. As shown in **Exhibit 4**, these states use similar approaches for providing internet access and ensuring the security of networks and devices, but they offer a range of examples of what types of devices are used and for which specific learning experiences. The profiles are intended to help other corrections leaders understand the policy and technical infrastructures in the four states and to consider the challenges and lessons learned for building state correctional education technology ecosystems. More research is needed, however, to understand the learner outcomes of these different uses of technology in correctional education programs.

EXHIBIT 4. SUMMARY OF PROFILED STATES' TECHNOLOGY COMPONENTS

State	Restricted Internet access	Security	Hardware and software	Funding sources for technology
Colorado	Wi-Fi in classroom only	Whitelisted within firewall by vendor	• Laptops • Secure networks • Secure videoconferencing hardware and software • Proprietary software • Open educational resources	• "Achievement earned time" (a form of performance-based funding that returns cost savings for sentence reductions to the state for educational uses) • *Workforce Innovation and Opportunity Act*, Title II • State general funds • Cash funds derived from sales revenue earned by the Canteen Operation and workforce programs
Louisiana	Wi-Fi in classroom and housing units	Whitelisted within firewall by vendor	• Laptops • Learning management systems	• *Elementary and Secondary Education Act*, Title I • *Workforce Innovation and Opportunity Act,* Title II • *Strengthening Career and Technical Education for the 21st Century Act* (*Perkins V*) • State appropriations • Justice Reinvestment Initiative funding • Second Chance Pell experiment
Maine	Wi-Fi in classroom and housing units	Whitelisted within firewall by college partners	• Tablets • Laptops • Learning management systems	• State department of corrections funds • Inmate benefit fund • Philanthropy, grants, university support, and donations
Wisconsin	Wi-Fi in classroom and housing units	Whitelisted within firewall by department of corrections	• Laptops • Interactive touchscreens • Operating systems • Videoconferencing hardware • Learning management systems • Student information systems	• *Elementary and Secondary Education Act*, Title I • State department of corrections appropriations • Second Chance Pell experiment • U.S. Department of Agriculture grants (for videoconferencing)

COLORADO DEPARTMENT OF CORRECTIONS

In 2014, the Colorado Department of Corrections (CDOC) created computer labs to support the transition from paper-based to computer-based GED testing.[5] This transition provided the opportunity for the state to adopt additional technology, such as laptops, for adult education and other education programs. Now more than 2,000 laptops are in use for adult education and college programs for a prison population of nearly 11,000 incarcerated individuals.

21
STATE CORRECTIONAL FACILITIES

3,770
ADULT EDUCATION STUDENTS

5,693
POSTSECONDARY EDUCATION, INCLUDING WORKFORCE TRAINING AND CTE STUDENTS

in 2019-2020

ECOSYSTEM HIGHLIGHTS: TECHNOLOGY

Multiple firewalls provide security for internet access.

Wi-Fi is available in both programming and housing units and can be controlled statewide from headquarters.

All adult education students have access to the same software package across the state using their laptops, which provides consistency and transferability of progress.

Students can earn industry-based certifications through applications accessed through Chromebooks.

Synchronous distance instruction is delivered to multiple prisons from a single location using videoconferencing cameras.

[5] The GED credential is a high school equivalency credential earned through passing the GED test, which is administered by GED Testing Service. See https://ged.com/about_us for more information on the GED test and credential.

ECOSYSTEM HIGHLIGHTS: INSTRUCTIONAL EXPERIENCES

Self-directed learning for adult education and CTE

Students can access a variety of CTE content on their own, including software for basic skills, employability skills, and high school equivalency content; courses and certifications in eight CTE subjects; and My Colorado Journey for career exploration. CDOC has identified content that relates to specific industries or general workforce preparation, can easily be secured, aligns with existing CTE courses, and addresses students' interests or requests.

Instructor-led synchronous postsecondary programs

Synchronous distance instruction is delivered to multiple prisons from a single location using videoconferencing cameras. Classes meet five days a week, with classes funded by Second Chance Pell Grants offered four days a week and other associate and bachelor's degree programs offered on the fifth day.

KEY ECOSYSTEM SUPPORTS

Access to education programs in the community

Students can access distance learning programs available in the community via laptops, such as an airline customer service class.

Access for remote prisons

CDOC has increased student access to college programs by providing instruction at remote prisons via videoconferencing.

CHALLENGES

The CDOC staff was concerned about potential misuse and damage to the laptops. Leadership developed policies and practices to address those concerns.

CDOC must coordinate with the Colorado Governor's Office of Information Technology to ensure that technology is approved and budgeted for use in correctional facilities.

LOUISIANA DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONS

When the high school equivalency exam became computer based, the Louisiana Department of Public Safety and Corrections (LDPSC) found a company that could create computer labs for students to take high-stakes tests and access academic software, and develop secure internet-connected laptops to alleviate concerns about classroom space and the limited course teaching schedule. With Wi-Fi in housing units, students can now access their coursework at any time at all state facilities.

8
STATE CORRECTIONAL FACILITIES

10+
SHERIFF-RUN JAILS

3,200
ADULT EDUCATION STUDENTS

900
POSTSECONDARY EDUCATION STUDENTS

~2,200
WORKFORCE AND CTE STUDENTS

in 2019-2020

ECOSYSTEM HIGHLIGHTS: INSTRUCTIONAL EXPERIENCES

Instructor-led asynchronous and synchronous postsecondary programs
Students can participate in a range of learning models. These include courses that are completely asynchronous, in which students access preset course content in the LMS, and others that include a combination of prerecorded materials and live virtual class sections.

Self-directed learning for adult education
In addition to in-class learning, adult education students have access to various education programs and resources via their tablets. These programs and resources are customized to the students' learning levels based on their placement test results and provide them with additional support in literacy, math, computer basics, and more. Students engage in a minimum of 15 hours of self-directed learning time per week, with the goal of preparing them to earn their high school equivalency degree.

CHALLENGES

Technology for educational use has expanded so quickly that DOC policy has not been created to support it.

Ensuring students feel like they are part of a college environment is difficult in online courses. Louisiana addressed this by requiring on-site college coordinators to work with online students.

ECOSYSTEM HIGHLIGHTS: TECHNOLOGY

LDPSC offers dual-boot stations, secure internet-connected computer labs in which students can access academic software and complete computer-based high school equivalency and industry certification exams.

LDPSC also provides laptops with access to colleges' LMSs.

Instructors use smart boards in classrooms at multiple facilities for synchronous distance and in-person instruction. Smart boards can also be accessed in computer labs and on tablets so that students can complete work on their own.

KEY ECOSYSTEM SUPPORTS

Pilot testing of the technology
LDPSC first piloted internet-connected computer labs at one facility and built support with security staff before expanding to laptops.

Training for instructors and staff
LDPSC offers a variety of training to faculty on how to use smart boards, laptops, and the full array of education and testing software. LDPSC also provides on-demand and individualized support to help instructors integrate technology.

State-level coordination
LDPSC hired a state-level educational technology coordinator to provide training, support implementation, and liaise with software and IT leads.

MAINE DEPARTMENT OF CORRECTIONS

In 2020, the University of Maine and Washington County Community College were selected to participate in the Second Chance Pell experiment. To support college-level work in the prisons, Maine Department of Corrections (MDOC) administrators supplied laptops to college students to match what students in the community used. Before this time, Maine had very little technology inside the prisons, and it has since grown from a few isolated computer labs to facility-specific resident education networks with laptops, tablets, videoconferencing, internet access, and LMSs to support all education programs.

6
STATE CORRECTIONAL FACILITIES

300 per year
ADULT EDUCATION STUDENTS

80 per year
POSTSECONDARY EDUCATION STUDENTS

in 2019-2020

ECOSYSTEM HIGHLIGHTS: TECHNOLOGY

College students use laptops in both classrooms and housing units and can access the college LMS for instructor-led asynchronous learning.

Students have real-time access to dozens of educational websites (see Appendix A for examples).

Carts with web conferencing equipment can be wheeled into different locations for instructor-led synchronous learning, in which instructors may broadcast classes to multiple facilities at once.

> **We started with secure lockdown networks and now we have some facilities with open Internet access. In the five years that we've really been pushing technology, we haven't had any major security incidents. We are building upon these proof points, and it's becoming second nature to use technology to support education programs.**
>
> — Ryan Thornell, Deputy Commissioner, Maine Department of Corrections

ECOSYSTEM HIGHLIGHTS: INSTRUCTIONAL EXPERIENCES

Instructor-led synchronous postsecondary programs

In partnership with local colleges, MDOC offers "inside-out online classes," in which incarcerated students enroll in college classes with students in the community. Courses are taught by college instructors via videoconferencing and meet one to two times per week. The instructors facilitate live discussion and online group work for academic courses and other "unconventional" classes, like Nonviolence as a Way of Life.

Self-directed learning for adult education

Adult learners use tablets that are loaded with more than 20,000 hours of educational content, including a differentiated literacy platform, books and videos, English language programs, and a personalized high school equivalency preparation program. Students also can access workforce preparation materials, such as career exploration and resume-building programs, and other life skills classes. Instructors may recommend certain programs to students based on their case plans, but the duration and intensity of engagement depends on the student and which program they select.

CHALLENGES

MDOC initially turned to a local networking vendor to help with implementation due to a lack of internal staff with the expertise to implement the technical infrastructure for education programming. Because the network and services were being built as they were being used, MDOC ended up with a patchwork of systems that are now being replaced with a more centralized and sustainable approach.

KEY ECOSYSTEM SUPPORTS

Supportive leadership and culture

MDOC's "culture of wellness" approach to corrections also applies to its use of technology and student access to the internet. MDOC sees value in using technology to promote rehabilitation and student responsibility.

Handling of security breaches on a case-by-case basis

MDOC holds individual students accountable for security breaches and misuse of the internet, rather than shutting down access for the entire facility.

State-level staffing

As the state moves to a more consistent approach to technology across facilities, MDOC has hired two dedicated staff for educational technology who will help standardize how the internet and other services are offered across facilities.

Consistent use of technology across facilities

MDOC convened a management committee of programs and service leaders in 2015. Any new practices or enhancements, including technology, are filtered through this committee to encourage consistency and support from stakeholders.

WISCONSIN DEPARTMENT OF CORRECTIONS

WISCONSIN 1848

Wisconsin Department of Corrections (WDOC) was developing a statewide student information system and educational network when Milwaukee Area Technical College (MATC) was selected to participate in the Second Chance Pell experiment. With few prisons close to MATC's main campus in Milwaukee, WDOC and MATC worked to expand technology options to virtually serve students throughout the state.

25
FACILITIES

2,388
ADULT EDUCATION STUDENTS

1,622
POSTSECONDARY EDUCATION STUDENTS
in 2020–2021

ECOSYSTEM HIGHLIGHTS: TECHNOLOGY

Every college student is authorized to use a laptop with access to a college LMS that can be used in classrooms and housing units.

....

Students can access whitelisted internet resources, including financial aid and employment websites (see Appendix A for examples).

....

MATC email accounts are created for students to complete the financial aid process via the whitelisted Free Application for Federal Student Aid® (FAFSA®) portal.

....

Through the statewide education network, WDOC's IT department can provide updated and consistent software across multiple facilities.

....

Computer labs provide access for all residents — not just those enrolled in education programs — to open educational resources through a separate portable server.

....

ECOSYSTEM HIGHLIGHTS: INSTRUCTIONAL EXPERIENCES

Asynchronous and synchronous instructor-led postsecondary programs

Students access pre-supplied content on the college LMS and complete assignments and quizzes on their own. They also receive virtual tutoring and participate in virtual office hours with instructors. College student services staff and faculty schedule videoconferences with students through local DOC education staff. Videoconferencing classrooms allow for broader access to classes that are broadcast from MATC's main campus to multiple prisons and provide more direct contact for students with instructors, tutors, and advisors.

CHALLENGES

MATC's LMS for its prison programs is limited to providing content to consume like recorded lectures and readings and not content to engage with like quizzes or discussion boards. LMS content for use in housing units must be downloadable. The LMS itself does not have an accessible offline version for use when not docked (in housing unit).

For security reasons, student laptops are used in "kiosk mode," which limits many functions, especially word processing.

> **We had slowly been growing our technology use for correctional education and it really took off with Second Chance Pell, enabling MATC to offer virtual and hybrid access to courses.**
>
> — Benjamin Jones, Education Administrator, Wisconsin Department of Corrections

KEY ECOSYSTEM SUPPORTS

Partnerships across education and IT

WDOC established a working group of educators and IT staff that meets monthly to ensure close coordination between the two departments. Senior leaders from both divisions also meet regularly.

Plans for student transfer

Wisconsin's statewide student information system allows easy access to student data after transfer.

Communication about technology needs

Over the course of the Second Chance Pell experiment, WDOC and MATC learned to improve communication and expectations around allowable technology for the prison environment. For example, when MATC decided it needed videoconferencing capability, confusion over which hardware would be allowed led to several delays and the incorrect purchase of equipment. The efficiency and efficacy of the overall system has improved by the establishment of roles in which MATC defines what it needs (e.g., videoconferencing, laptops, library resources, simulators) and WDOC identifies which technology can securely meet those needs.

Lessons Learned

All four states addressed seven key topics when developing their correctional education technology ecosystems: security, funding, staffing and teacher development, student development, instructional approaches, instructional devices and resources, and vendor selection. Across these topics, the following themes emerged as important considerations for building the necessary ecosystem support and expanding technology use for correctional education:

- **Gaining leadership support and designing reasonable security protocols that promote student responsibility.** All four states noted that strong support from DOC leadership was critical for navigating security requirements to provide access to and expand the use of educational technology. At least two states described a shift in security protocols to focus on individual, rather than systemwide, consequences. They described the need for advanced and ongoing planning to anticipate and address any potential misuses of technology, such as by simulating hacks and developing flexible policies at the state and facility level.

- **Using multiple funding sources to support technology use.** All four states used a variety of federal, state, and private funding sources to support technology use, and described the importance of cross-agency partnerships to leverage monetary and in-kind resources.

- **Having dedicated staffing for coordinating educational technology use statewide.** In all four states, the vision for using educational technology typically originated with the state correctional education director, who also had responsibility for executing this vision. State administrators described the need for additional state-level staff to coordinate the day-to-day technology duties, which range from purchasing devices to providing training and technical support and emphasized the need for staff with expertise and an understanding of both education programs and IT systems.

- **Adopting technology to help students develop or improve digital literacy skills, especially in preparation for reentry.** The four states varied in their approaches to introducing students to technology, with one state relying on technology "by immersion" and others teaching technology basics. However, they all emphasized the crucial need to ensure digital equity by preparing students to participate in technology-supported instruction, whether while incarcerated or after release, and helping students develop the skills needed to navigate technology in their everyday lives upon reentry.

- **Selecting the right device, modality, and vendor for the right program or purpose.** All four states use a combination of education devices and platforms that include tablets, laptops, and computer labs and that were provided or supported by a variety of vendors. Different devices might be used by different education levels or for different instructional activities. At a minimum, correctional education leaders should talk with education providers and vendors to make sure that whatever devices are selected reflect those being used in the community to prepare students for success after release.

- **Understanding instructional strategies for using technology in the community that can be applied to correctional education.** While the research base on the use of educational technology in corrections is limited, all four states used a range of instructional approaches that addressed their instructional needs and reflected best practices for using educational technology in the community. These included in-person and distance learning experiences that encouraged student collaboration and problem-solving using different digital tools.

DISCUSSION GUIDE

The following discussion guide focuses on the seven key ecosystem supports identified in the Lessons Learned: security, funding, staffing and teacher development, student preparation, teaching and learning, device selection, and vendor selection. It provides a summary, implications for policy and practice, and discussion questions for each area. State correctional education and IT leaders can use the discussion guide to reflect on their current use of educational technology and/or identify plans to expand usage.

Before you Begin: Develop an Evaluation Strategy

As states adopt or expand educational technology, they should intentionally consider how to evaluate the use of technology in correctional education programs from the start. Evaluation spans the seven topics included in this discussion guide and involves identifying and measuring the outcomes that state agencies would expect to see because of technology use. These outcomes might range from specific learning milestones to access to educational content, behavior or morale improvement, and increased digital literacy skills. Outcomes might also include post-release measures, such as enrollment in additional education programs or employment.

SECURITY

RECOMMENDED AUDIENCE

IT leaders; DOC security staff, including superintendents and wardens; and education leaders

Security considerations include both the cyber and physical infrastructure (e.g., the hardware and software) needed to connect students and instructors and provide access to online educational content and the physical space where learning takes place. Specific security concerns may include potential misuse of devices, access to sensitive data, or improper communication. To alleviate security concerns, many state DOCs place limitations on access to information and devices, such as providing restricted internet access or whitelisting certain websites within the state or vendor's firewall (see Appendix A for state whitelisting examples).

As technology use expands in correctional education, corrections administrators must consider strategies for securely providing technology access and identify policies for addressing security breaches. States handle security breaches in different ways that range from shutting down the whole educational technology infrastructure (and discontinuing use for all students) to removing access for just those students responsible for any breaches. Some states have developed specific educational technology and program internet use agreements that must be understood and signed by the students before they can access the internet. The agreement can specify the purpose for the educational technologies and internet use per student. States have also created educational technology standard operating procedures (SOPs) that include specific details like the physical layout of a computer lab and procedures to store laptops and tablets. SOPs also can include procedures for monitoring student internet use with real-time monitoring applications and scheduled audits of devices and browser history. Appendix B includes an example of a state SOP for educational technology.

Federal Security Standards

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations and risk assessment for cloud computing technologies. In other words, it offers a model for federal agencies interested in streamlining security protocols for internet use. See the FedRAMP website for guidance, templates, and best practices for designing security controls (https://www.fedramp.gov).

Implications for Policy and Practice

- Engage IT leaders — within the DOC and other state agencies — in early conversations about technology adoption to ensure broad agency buy-in and to address both education and security needs up front.

- Communicate security needs with any potential vendors to understand how they will ensure compliance with security requirements and provide ongoing security support.

- Plan time for any potential security issues, discuss with state and facility leaders how these issues will be addressed, and develop new or additional security documentation on how to handle electronic breaches internally and/or externally.

- Develop SOPs that document security procedures for dealing with educational technologies and develop an educational technology or internet use agreement for students that documents the specific purpose and use of educational technology and/or the specific program being accessed via the internet.

Discussion Questions

1. What DOC security protocol requirements does the selected educational technology have to meet? If there are no security requirements, who is responsible for developing the security requirements, policies, and SOPs?

2. Who is responsible for the security of devices or software (i.e., ensuring students are restricted to specific content)?

3. Who is responsible for testing the software and hardware for security issues?

4. Are there specific physical security requirements for laptops and tablets? For example, should devices be ruggedized (i.e., protected to make them unbreakable), rubberized, or have clear cases? Should security screws be used in the case? What are the requirements for storage and charging?

5. What happens if security is breached?

6. How will user data be protected?

7. How will access to the Internet be provided?

8. Where will users be able to access devices?

9. Who will provide technical IT security support (e.g., educational partner, technology vendor)?

FUNDING

RECOMMENDED AUDIENCE

DOC education leaders and college administrators

To fund the adoption of instructional technology for correctional education, state agencies should consider both the initial and ongoing costs of the technology, which includes hardware and software, and identify sufficient fiscal resources to cover the costs. Generally, states do not have line items in agency budgets to fund educational technology and instead rely on multiple funding sources. These sources include state and federal education funds, state and federal corrections funds (such as Justice Reinvestment Funds), and grants from private foundations. For example, technology for use in adult education programs might be funded by a combination of *Workforce Innovation and Opportunity Act* Title II funds and state adult education dollars. For postsecondary programs, technology costs often are covered by college funds and/or through technology fees charged to revenue from the Second Chance Pell experiment.

Most states patch together a variety of funds to purchase instructional technology and cover any associated costs, such as annual licensing fees, vendor subscriptions, and software. These costs may be short and long term and include direct and indirect expenses (U.S. Department of Education 2015).

Common Funding Sources for Correctional Education

Many states leverage funding from a variety of federal and state sources to administer correctional education programs and support use of technology in programs. These sources include the following:

Federal
- *Adult Education and Family Literacy Act* formula grants to states (Title II of the *Workforce Innovation and Opportunity Act*)
- *Strengthening Career and Technical Education for the 21st Century Act (Perkins V)*
- Second Chance Pell experiment*
- Grants under the Second Chance Reauthorization Act of 2018

State
- *State corrections appropriations*

*In December 2020, Congress reinstated eligibility for federal Pell Grants for incarcerated students.

Implications for Policy and Practice

- Look for innovative funding sources like achievement earned time (i.e., costs saved when sentences are reduced for completion of education programs), that can contribute to technology costs.

- Be prepared to braid funding from multiple sources to purchase and support technology as needs arise and on an ongoing basis.

- Consider the ongoing and indirect costs, like staff training and professional development, that accompany the purchase of hardware and software.

- Develop a replenishment plan for purchasing updated technology over time (e.g., every three to five years) to ensure it remains current and aligned with state needs.

- Establish policies that seek to avoid charging students for devices or ensuring available aid to cover the costs of such devices, and consider the impact on equity.

Discussion Questions

1. Will the technology be purchased or rented?

2. What funding sources are available to pay for technology?
   - Which department(s) or agency(ies) is paying for the technology?
   - Will this department or agency also be responsible for maintaining the technology?

3. How much does the technology (hardware and software) cost, and what do the costs cover?
   - Is it a one-time or ongoing charge?
   - How do these costs compare across different vendors?

4. How will other associated costs (e.g., staff training, IT support, evaluation) be covered?

5. Are students charged for the devices and use of specific educational software? If so, how? With equitable access in mind, how will students enroll and participate should they not be able to pay?

6. What funding sources will be available for future technology purchases?

7. What are the necessary procurement processes for using these funds? What are the procurement timelines for these purchases?

STAFFING AND TEACHER DEVELOPMENT

RECOMMENDED AUDIENCE

DOC education leaders, correctional officers, college administrators, and instructors

Technology coordination support may be drawn from multiple staff and/or departments, such as education and IT, and requires knowledge of both education and technology systems. Often this role falls by default to the state correctional education director on top of all their other responsibilities. Therefore, some states hire technology coordinators specifically for education to oversee day-to-day responsibilities, which include selecting, purchasing, and distributing hardware and software; managing and implementing security protocols; troubleshooting network or device issues across facilities; and supporting the integration of technology into instruction.

Additionally, instructors must both be familiar with the technology themselves and be trained in effective strategies for integrating technology into instruction (see text box). Some training is provided by device or software vendors and may address both needs. State agencies also provide training, either on an as-needed basis or in a more formalized structure, and other resources, such as access to digital instructional materials to enhance classroom instruction and opportunities for networking with other teachers to discuss technology use.
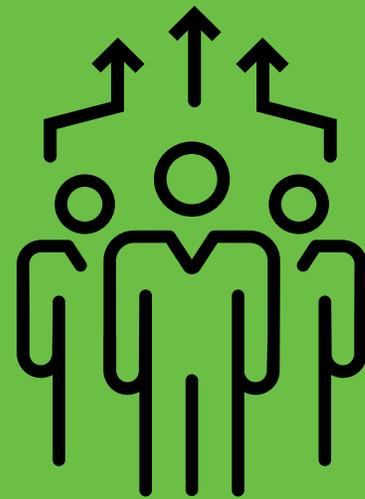
Common Standards for Technology Integration

Correctional education programs can draw from the evidence base on effective strategies for integrating technology into instruction that has been identified for K–12 education. Two examples of this evidence base include:

- International Society for Technology in Education Standards for Educators (https://www.iste.org/standards/iste-standards-for-teachers), which outlines seven standards to help teachers develop the digital skills and understand instructional approaches for integrating technology into their practice; and

- Technology Integration Matrix (https://fcit.usf.edu/matrix/matrix), which provides a framework for integrating technology into instruction that includes active, collaborative, constructive, authentic, and goal-directed strategies.

Implications for Policy and Practice

- Designate a state educational technology coordinator who can work with both IT and education staff to support safe and effective uses of educational technology.

- Develop a plan for providing instructors with training and resources to help them effectively use technology and update staffing policies, as necessary, to reflect technology training needs.

- Hire staff at both the state and facility levels who have experience using educational technology and consider a coaching approach for professional development to pair more experienced technology instructors with new users.

- Update hiring policies to establish expectations for staff training and qualifications related to educational technology.

Discussion Questions

1. Who will serve as technology coordinator at the state level? Will this be a dedicated position or a shared responsibility?

2. What professional development opportunities does the state provide to correctional education staff on using educational technology?

3. What other professional development opportunities, such as training provided by a vendor, or resources are available?

4. What other needs does the staff have for professional development on using educational technology?

5. How will teachers help evaluate technology use?

STUDENT PREPARATION

RECOMMENDED AUDIENCE

DOC education leaders, college administrators, instructors, and students

Providing access to current technology to incarcerated students is an important equity and reentry issue. Technology can be a vital tool in lifelong learning. Technology skill development is critical to preparing students for success after release given the prevalence of technology use in society. Participants in correctional education programs may have different levels of familiarity with current technology based on their age, background, level of education completed, length of time incarcerated, and other factors. Therefore, to benefit from technology-enabled instruction, some students may need additional support to help them learn to use and apply different digital devices and platforms. Key digital competencies include digital literacy, basic computer skills, digital problem-solving, and information literacy (ISTE, 2016; Vanek, n.d.). Correctional education programs can help develop these competencies by offering digital literacy courses, supporting self-directed online learning opportunities, integrating technology into education programs, and providing regular access to technology. Some states are adopting digital literacy certifications for students in correctional education programs to verify their understanding of digital literacy and the impact of technology on students' lives.

Digital literacy skills are those "**skills associated with using technology to enable users to find, evaluate, organize, create, and communicate information; and developing digital citizenship and the responsible use of technology**" (definition in *Workforce Innovation and Opportunity Act* adopted from the Museum and Library Services Act of 2010, Pub. L. 111-340, Dec. 22, 2010).

Implications for Policy and Practice

- Develop or adopt digital literacy standards or frameworks for correctional education programs. Many states already have such frameworks for adult education or K–12 education that could be adapted for correctional education.

- Identify what technology is being used by education programs and employers in the community.

- Provide access to technology both in the classroom and in housing units to give students opportunities to practice using technology and improve their digital literacy.

- Convene students to gather their feedback on the use of technology in education programs.

Discussion Questions

1. How will the state ensure that students are ready to use technology for educational purposes?

2. Does the agency (or other state agencies) have standards for digital literacy that could be used in correctional education programs?

3. What support will the state provide to develop students' familiarity with different technology and increase their digital literacy skills?

4. For computer-based assessments, what opportunities will students have to use computers before taking the assessment?

5. How will the state ensure that students have access to the technology being used for education programming in the community?

6. How will the state monitor the quality of online and digital resources that will be accessible to students?

7. When and where (e.g., housing units, classrooms) will students have access to technology?

8. What opportunities do students have to engage with current technology outside of education programs (e.g., for work experiences or personal use)?

9. How will the state evaluate the approach to developing student readiness for technology use?

TEACHING AND LEARNING

RECOMMENDED AUDIENCE

DOC education leaders, college administrators, instructors, and students

Technology is being used across levels in correctional education programs, including adult basic education, CTE, and postsecondary education, and it supports a variety of teaching and learning experiences, such as instructional delivery models and assessment. For technology to be used effectively, it must be used in conjunction with evidence-based, quality instructional approaches, and it should help students meet their learning goals. States should regularly evaluate the quality of technology-supported instruction in correctional education programs to assess the extent to which technology is enhancing teaching and learning environments.

There is no one-size-fits-all approach when it comes to technology-supported instructional models for correctional education. Historically, correctional education has been delivered through an instructor-led, synchronous, in-person approach, but this is changing with the use of educational technologies.

The appropriate learning model or combination of models for a particular education program depends on several factors, including providing the best method for content delivery, scheduling, instructor availability, classroom space, internet access, and the digital literacy skills of teachers and students. Decisions about which models to use should be driven by student learning needs, especially related to their digital literacy skills. Technology should be integrated using evidence-based practices, which focus on active and authentic uses of technology that included project- or inquiry-based learning.

Implications for Policy and Practice

- Develop digital equity and inclusion plans that describe how instructional strategies will help reduce barriers to technology use and access for all students.

- Ensure teaching and learning strategies and goals drive decisions about what educational technology to select. Educational technology should enhance or support student learning.

- Develop a student-centered educational technology ecosystem that allows access to educational content in multiple settings (e.g., from housing units to the classroom) and encourages collaborative learning.

- Align instructional modalities with other components of the educational technology ecosystems, including the physical and technological infrastructure.

- Be innovative and flexible to allow modalities to shift as learner and program needs evolve.

Discussion Questions

1. How will the education provider use the technology to support or develop a learning community of students?

2. What courses are most difficult to teach with technology, and how will technology allow for those courses to be enhanced?

3. Is the technology being integrated in an adequate way to help students reach the learning outcomes of the education program?

4. How will the technology support assessments?

5. How will the technology support and improve existing face-to-face instruction?

6. How will the technology support and improve distance learning?

DEVICE SELECTION

(DESKTOPS, LAPTOPS, AND TABLETS)

RECOMMENDED AUDIENCE

DOC education leaders, college administrators, instructors, and students

In 2015, most states provided access to technology in computer labs located in education departments. Access to internet resources, whether directly through whitelisting or through local hosting, was rare. States now provide educational technology with laptops and tablets in addition to computer labs. This has allowed expanded access to educational services from classrooms and labs to housing units and dayrooms. Key factors in deciding which type of device to use often involve software choices, security concerns, and ease of implementation. The trade-offs of using different types of devices are summarized in **Exhibit 5**. See Appendix C for examples of common technology vendors for corrections.

EXHIBIT 5. SUMMARY OF ADVANTAGES AND DISADVANTAGES FOR EDUCATIONAL TECHNOLOGY DEVICES USED IN CORRECTIONAL EDUCATION

Device	Advantages	Disadvantages
Desktops	· Can run a full suite of software, including graphics-intensive programs · Easy to secure on wired networks with simple oversight	· Limited to classrooms and computer labs · Difficulty providing a desktop for every student due to cost and space limitations
Laptops	· Can be used in housing units and dayrooms · Can run most software used on desktops	· High cost · Complicated physical and network security · Limited battery life
Tablets	· Often already available under vendor contract for entertainment and email purposes · Can be used in housing units and dayrooms · Low cost	· Limited suite of software · Complicated physical and network security · Small size that can limit use for complex tasks (like word processing) · Limited battery life

Implications for Policy and Practice

- Identify the purpose of the device. No single device — desktop, laptop, or tablet — meets the needs of all educators and learners. For example, college-level courses that require typing and data entry may be better served with laptops, while adult education courses that include reading and watching lessons may be better served with tablets.

- Bring educators, security, and IT staff together to determine which devices will meet the needs of learners and instructors while meeting security requirements.

- Develop or update state policy on technology use to address needs for different devices by different education programs.

Discussion Questions

1. What devices are used or recommended by the education provider for what purpose/type of instruction?

2. What devices are used by students participating in similar education programs on the outside?

3. What types of academic tasks do students need to perform on the device (e.g., email, reading documents, watching lectures, writing reports)?

4. Does each student need their own device?

5. Who "owns" the device (e.g., the facility, program, or student)?

6. What happens if the device breaks?

7. If the facility has a computer lab, is the lab available at hours that students can access it? Who supervises the computer lab? Is staff available for enough hours that students can complete their work?

8. How will students submit their assignments? How will education providers update content?

VENDOR SELECTION

RECOMMENDED AUDIENCE

DOC education leaders, DOC IT staff, DOC procurement, college administrators with input from instructors and students

States may choose to develop technology in house, or they may opt for vendor services for some or all technology needs. Vendors can offer options for devices (tablets, laptops, and computer labs), videoconferencing, LMSs, and other educational technology, and states should carefully review how a vendor's product aligns with education programming needs and goals. States select vendors for different reasons, but key considerations typically center on security, cost, and compatible software applications. In addition to the specific products, state corrections agencies should also consider the customer services offered by the vendor, such as training on the products and being available to answer questions.

Vendor Selection Examples

States choose vendors based on several factors. In some cases, tablets for email and entertainment can be adapted for distance education. Other states choose vendors that provide devices specifically for education; students in these states might have two devices— one for entertainment or email and the other for educational purposes. Because some states prohibit incarcerated people from accessing the state network, some DOCs select vendors to provide separate network access. Finally, other states look for custom-built devices to meet stringent security requirements.

Implications for Policy and Practice

- Do research to ensure the vendor is providing the solution that is needed.

- Have faculty and students test devices and applications before finalizing purchase. Educational technology is a long-term commitment, and it is important to pilot devices to ensure they will provide the service that is needed.

- Establish policy and procedures for handling student data and ensure that vendors comply with state requirements.

Discussion Questions

1. What is the vendor's licensing model? Are the device and software provided as a service with an annual fee or is it a one-time cost?

2. What educational applications or software can be accessed or are loaded on the device? Who selects which applications are available to faculty and students?

3. How much does the device cost? What is the total cost of the device over its lifetime?

4. What types of technical support and training does the vendor provide?

5. How is the device's security ensured?

6. What information does the vendor provide about student progress or usage?

7. How does the device or software handle student-level data?

NEXT STEPS AND RECOMMENDATIONS

Educational technology use in corrections is rapidly expanding to improve digital equity for students, provide high-quality education services, and prepare students for success after release. In just more than five years, "early adopters" of technology for correctional education have evolved from technology use in single institutions to multiple facilities across their states and across multiple education levels. Expanding use of educational technology is an important start, but it also requires ongoing attention to state policy, technical considerations, and staffing to ensure that technology is safely used to improve the quality of instruction and learning.

States also must develop strategies to ensure equitable access to high-quality educational technology within facilities and across education levels. This includes allowing access to devices and the internet in both housing units and classroom spaces to ensure students have sufficient opportunity to engage with educational content and develop their digital literacy skills. It also involves identifying strategies to ensure students can use devices at no cost to them to eliminate barriers to access.

Education providers and vendors continue to innovate and adopt new technology for the corrections environment. This brief focuses on the technology needed to conduct class in today's context, but some correctional education programs are using more innovative and emerging technology. Several education providers have begun to use augmented reality and virtual reality in CTE instruction, such as automotive repair and computer coding. Others have introduced advanced manufacturing practices, such as 3D printing and computer-aided design and manufacturing.

Library services continue to expand, and at least two library database vendors are now offering widespread access to journals and academic databases normally limited to college campuses. Finally, communication tools and LMSs are rapidly evolving to connect instructors, counselors and advisors, reentry navigators, and financial aid staff with students inside prisons.

With Congress incorporating Pell Grant restoration for people in federal and state prison facilities enrolled in qualifying prison education programs (to take effect in mid-2023) in the F*AFSA Simplification Act*, colleges and universities are poised to establish new programs and expand existing programs to a scale that has not been seen since 1994. In recent years, the Second Chance Pell experiment tripled in size from 65 colleges in 2016 to 200 colleges for the 2022–23 school year. Many of these colleges have learned to use financial aid to increase access to technology for students. As more colleges begin operating in prisons, there will be increased pressure, and new resources, to provide current educational technology to learners and instructors inside correctional facilities.

As technology use continues to rapidly expand, corrections leaders will need to support such expansion intentionally and thoughtfully, with a focus on selecting high-quality products and using evidence-based practices for integrating technology into instruction. This research base does not currently exist in corrections, so lessons learned from research outside of corrections can continue to be applied until more concrete information is known about the specific devices, platforms, and instructional models that best support technology use in correctional education.

Recommendations for Field

To ensure high-quality, equitable access and use of educational technology, the corrections field should consider the following:

- **Support ongoing and expanded access to high-quality educational technology in correctional education**: To improve digital equity among incarcerated individuals and better prepare them for full participation in society, all correctional education students must have the opportunity to use technology to support their learning. States can support such access and use of technology by identifying funding sources, providing training to staff, partnering with IT staff to address security requirements, developing appropriate technology policies, and evaluating technology use in correctional education programs.

- **Provide dedicated IT staff for correctional education**: DOC IT staff play a key role in expanding access and scale to educational technology, especially in partnership with DOC education staff. While they may bring different perspectives and priorities, both education and IT staff can play a role in addressing security requirements and meeting programming needs for technology. Hiring state-level staff dedicated specifically to supporting IT needs for correctional education

programs could help bridge these cross-agency partnerships and alleviate burdens on state education staff. Additionally, conversations within state agencies and across the country, such as roundtable discussions among educators and IT leaders, could help to advance conversations about strategies for overcoming security limitations within correctional facilities.

- **Increase technical assistance for staff**: Each state creates its own security protocols for internet use, leading to inconsistent access across states. State agencies could look to the Federal Risk and Authorization Management Program (FedRAMP) model and other federal strategies as examples of how the federal government established a standardized approach to security practices for cloud service offerings. Before FedRAMP, technology vendors had to meet different security requirements for each federal agency. FedRAMP provides a common security framework across federal agencies.

- **Increase technical assistance for staff**: Each state creates its own security protocols for internet use, leading to inconsistent access across states. State agencies could look to the Federal Risk and Authorization Management Program (FedRAMP) model and other federal strategies as examples of how the federal government established a standardized approach to security practices for cloud service offerings. Before FedRAMP, technology vendors had to meet different security requirements for each federal agency. FedRAMP provides a common security framework across federal agencies.

- **Provide technical assistance to education providers and other DOC staff on FERPA and other privacy issues for the use of technology**: Throughout vendor and state interviews conducted for this brief, a need for more information about the impact of educational technology on student and user data became clear. Both sets of stakeholders would benefit from additional training on their responsibilities to ensure the privacy of individual users, including FERPA protections. Such clarity might be provided through technical assistance on how FERPA works within the correctional education classroom and especially with third-party technology providers.

- **Evaluate what works in educational technology**: No widespread evaluation of the use of educational technology in corrections exists. The few evaluations that have been completed do not meet research standards. More research is needed to assess the quality of different technology-supported instructional models as well as the use of different devices and/or learning platforms. In short, while the use of educational technology is rapidly expanding, the field needs more guidance on what technology to use and how best to use it.

GLOSSARY

Active Directory: A Microsoft technology that helps organize and manage computers and other devices on a network. It allows network administrators to create and manage user accounts.

Asynchronous distance learning: A form of virtual instruction that does not require students and instructors to be in the same place or participate in classes at the same time. Instead, students access educational content on their own time and from any location.

Cybersecurity: The protection of digital assets from unauthorized use or access by a combination of people, policies, processes, and technologies.

Database: A structured collection of information or data typically stored electronically. The most common types of databases store data in rows and columns in a series of tables to make processing and data querying more efficient.

Data infrastructure: The technology, processes, and people needed to collect, store, maintain, distribute, and use data.

Digital citizenship: Using computers, the internet, and digital devices responsibly to participate in society.

Digital literacy: The skills needed to use technology to find, consume, and create information and to develop digital citizenship.

Family Educational Rights and Privacy Act (FERPA): A federal law that protects the privacy of student education records. The law applies to education agencies and institutions that receive funds under programs administered by the U.S. Department of Education.

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software or a combination of both.

Hardware: The physical machinery and devices that make up a computer system.

Internet Service Provider (ISP): A business or private-sector organization that provides access to the internet.

Isolated local server: A server that is connected in an environment with no connection to any other network, including the internet.

Kiosk: An interactive, unattended, self-service computer terminal available for public use. It can be used both to charge laptops and tablets and to allow for data transfer that may not be permitted when a device is not connected to the kiosk. Data are then available for offline viewing once the device is disconnected from the kiosk.

Learning management system (LMS): A software application for the administration, documentation, tracking, reporting, and delivery of virtual education courses or training programs.

Local area network (LAN): A group of computers and other devices dispersed over a relatively limited area and connected by a communication link that enables a device to interact with any other on the network.

Network: A system that includes communication capability that allows one user or system to connect to another user or system and that can be part of a system or a separate system. Examples of networks include local area networks or wide area networks, including public networks such as the internet.

Open educational resources: Teaching, learning, and research resources that reside in the public domain or have been released under a license that permits their free use, reuse, modification, and sharing with others. Digital openly licensed resources can include complete online courses, modular digital textbooks, and more granular resources, such as images, videos, and assessment items.

Operating system: The software that communicates with and supports the basic functions of a computer and manages the computer hardware.

Physical infrastructure: The space where technology is used, and the tools needed to maintain it (e.g., servers, computer labs, Wi-Fi routers, chargers, and docking stations).

Point-to-point secure line: A private data connection securely connecting two or more locations to allow for secure internet access from a server.

Restricted internet connection: A connection that limits internet access to preapproved content through use of firewalls and routers. Allowable internet content must be whitelisted, and all other hardware and software must be removed from devices.

Self-directed learning: A learning model in which students participate independently in a virtual education program or course. Students access online content and resources on their own and complete coursework at their own pace.

Software: A collection of instructions, data, and programs that enable a computer to operate. It includes all the information processed by the computer systems, including programs and data.

Student data: Information collected on individual students, including personal information (e.g., a student's age, gender, race) and enrollment and other academic information.

Student information system: A school administration software system used to manage student-related data, such as for documenting grades, registering students in courses, tracking assessment scores, recording student attendance, and creating class schedules.

Synchronous distance learning: An instructional model that relies on instructor(s) and students(s) to connect virtually at the same time for learning to take place.

Whitelisting: The development of a list of trusted entities, such as applications and websites, that are exclusively allowed to be accessed and function within a network.

Wide area network (WAN): A computer network that connects geographically separated areas and provides a more secure means of transferring data than the public internet.

Wi-Fi (wireless fidelity): Networking technology that allows computers and other devices to communicate over a wireless signal.

Wireless network: A network that allows devices to connect and communicate wirelessly, rather than over ethernet cables.

REFERENCES

Constantakis, Patti. 2016. *Designing Technology for Adult Learners: Applying Adult Learning Theory*. Washington, DC: Digital Promise. https://digitalpromise.org/wp-content/uploads/2016/03/designing-for-adult-learners.pdf.

Darling-Hammond, Linda, Molly B. Zielezinski, and Shelley Goldman. 2014. *Using Technology to Support At-Risk Students' Learning*. Washington, DC: Alliance for Excellent Education. https://edpolicy.stanford.edu/sites/default/files/scope-pub-using-technology-report.pdf.

Edutopia. 2007. "How to Integrate Technology." https://www.edutopia.org/technology-integration-guide-implementation.

Escueta, Maya, Vincent Quan, Andre Joshua Nickow, and Philip Oreopoulos. 2017. *Education Technology: An Evidence-Based Review*. NBER Working Paper 23744. Cambridge, MA: National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w23744/w23744.pdf.

ISTE (International Society for Technology in Education). (2016). "ISTE Standards: Students." https://www.iste.org/standards/for-students.

Reich, Justin, and Mizuko Ito. 2017. *From Good Intentions to Real Outcomes: Equity by Design in Learning Technologies*. Irvine, CA: Digital Media and Learning Research Hub. https://clalliance.org/wp-content/uploads/2017/11/GIROreport_1031.pdf.

Rosen, David J., and Jen Vanek. 2020. *The What, Why, Who, and How of Blended Learning for Adult Basic Skills Learners*. Syracuse, NY: New Readers Press. https://www.newreaderspress.com/site/Additional%20Resources/ProLiteracy_BlendedLearningGuide_2020-11.pdf.

Tanaka, Kurtis, and Danielle Cooper. 2020. *Advancing Technological Equity for Incarcerated College Students: Examining the Opportunities and Risks*. New York: Ithaka S+R, May 7. https://doi.org/10.18665/sr.313202.

U.S. Department of Education. 2015. Notice Inviting Postsecondary Educational Institutions to Participate in Experiments Under the Experimental Sites Initiative. 80 Fed. Reg. 45,964–45,966 (August 3, 2015). https://www.govinfo.gov/app/details/FR-2015-08-03/2015-18994/context.

U.S. Department of Education, Office of Career, Technical, and Adult Education. 2015. *Educational Technology in Corrections: 2015*. Washington, DC: U.S. Department of Education. https://www2.ed.gov/about/offices/list/ovae/pi/AdultEd/policybriefedtech.pdf.

U.S. Department of Education, Office of Educational Technology. 2017. *Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update*. Washington, DC: U.S. Department of Education. https://tech.ed.gov/files/2017/01/NETP17.pdf.

Vanek, Jenifer. n.d. "The Skills That Matter in Education." Issue Brief: Digital Literacy. Arlington, VA: American Institutes for Research. Accessed August 16, 2021. https://lincs.ed.gov/sites/default/files/TSTMDigitalLiteracyBrief-508.pdf.

Vanek, Jenifer, Destiny Simpson, and Jeff Goumas. 2020. *IDEAL Distance Education and Blended Learning Handbook*. 7th ed. EdTech Books. https://edtechbooks.org/ideal_dl_handbook.

SAMPLE WHITELISTED WEBSITES

The following are examples of websites that are commonly whitelisted by state departments of corrections for educational purposes. The web addresses for these sites can be found by entering the titles into a search engine. Note that some of the websites may be listed in multiple categories.

Secondary-Level Education or High School Completion

- Acellus
- Aztec Software
- Essential Education — GED Academy
- Houghton Mifflin
- Immerse2Learn

Job Search and Reentry

- My Colorado Journey
- My Virtual Job Shadow
- Wisconsin's America Job Center

Learning Management Systems

- Canvas
- Blackboard
- Brightspace
- Google Classroom

Library Services

- EBSCO
- JSTOR

Testing and Certification

- ESCO Testing
- National Center for Construction Education and Research
- Pearson VUE

Workforce Training

- Acellus
- Aztec Software
- CISCO Netacademy
- Essential Education – GED Academy
- iCEV
- Tooling U-SME

SAMPLE STATE OPERATING PROCEDURES FOR TECHNOLOGY USE (MAINE DEPARTMENT OF CORRECTIONS)

The following sample state operating procedures were provided by the Maine Department of Corrections as an example of how the agency has operationalized technology use.

STATE OF MAINE
DEPARTMENT OF CORRECTIONS
BOLDUC CORRECTIONAL FACILITY

JANET T. MILLS

GOVERNOR

Standard Operating Procedure (SOP)

Department/Area: BCF   **SOP Number:**

Subject: Education Program internet Usage, Supervision and Monitoring

Effective Date: **Last Revision Date:**
_____

Procedure: Education Program internet Usage, Supervision and Monitoring

Purpose: Per **Policy 24.10, Prisoner Use of Computers and/or Access to the internet**, approved clients are allowed to use Department computers and/or access authorized resources on the internet to enhance education in adult facilities.

This Standard Operating Procedure (SOP) is to ensure that access to computers and/or the internet is carried out in a transparent and consistent manner, that is securely and routinely monitored and audited.

SOP Contents

Classroom Setup

- The classroom shall be set up so that all computer screens are visible from at least one window in the classroom. This will allow for officers and other staff to see all computer screens at the same time and to do routine and random checks of computer and/or internet.

Internet Use

- All students who have been approved to use computers and/or the internet as part of their educational plan, must sign the computer use agreement (Policy 24.10, Attachment B). The BCF teacher will make sure each student has an updated computer use agreement in their education file.
  - Each computer use agreement should specify the exact purpose for internet use (i.e., Student A is using the internet as part of their Second Chance Pell courses)
  - If staff have questions about approved website access, the BCF teacher should be consulted.

- All students enrolled in education programming that requires computer and or/internet access will be assigned an account on the Active Directory (AD). Each student will have a personalized log in and password. Any laptop activity will be linked to individual students. Students shall not share login information and will be held accountable for any activity that happens on their AD account.
- Only laptops set up on the AD will be allowed to access the internet.
- Access to the internet is limited by an approved list of websites.
- When students leave the classroom, they must log off their AD account.

Schedule and Supervision

- The classroom will be open for internet use Monday through Friday 9:00 a.m. to 9:00 p.m. and Saturday and Sunday from 11 a.m. to 5:00 p.m. During normal and unscheduled lockdowns, the classroom will be shut down.
- Per Policy 24.10, Prisoner Use of Computers and/or Access to the internet:

  > *Designated education staff or the case manager, as appropriate, shall monitor computer use and/or internet access by the prisoner to ensure appropriate use. Security staff may monitor computer use and/or internet access by the prisoner to ensure appropriate use. As part of the monitoring, staff may inspect a computer, a USB drive/flash drive, electronic files, downloaded or printed material, internet sites accessed, etc. at any time for any reason.*

- There is no requirement for direct supervision of students accessing the internet. The BCF teacher will be present in the education classroom during as many hours Monday through Friday that he/she is available. Officers will make every attempt to do hourly and random checks in the classroom during internet usage time all days of the week and on all shifts, as applicable.

General Monitoring/Auditing

- *Per Policy 24.10, as part of the monitoring, staff may inspect a computer, a USB drive/flash drive, electronic files, downloaded or printed material, internet sites accessed, etc. at any time for any reason.*
- The BCF CAO, or designee, will set a schedule and process for:
    o Monitoring computer and/or internet usage;
    o Examining the educational technology hardware (such as laptops, flash drives, printers, etc.); and
    o Auditing information contained within the hardware (i.e., reviewing files on the flash drive, documents on the computer, websites access, email accounts, etc.).

- Monitoring should be done by a variety of staff on all shifts.
- Monitoring should be done at scheduled and random times.
- At a minimum, monitoring/auditing should be done at least three times weekly.

Website Adding and Monitoring

- BCF staff, through authorization from the CAO, or designee, will be able to add approved educational websites to the whitelist.
- The video and instructions on how to add websites to the whitelist is available through a shared BCF drive. The Assistant Director can be consulted for video access.
- The BCF CAO, or designee, will create a schedule and process for reviewing website access for every active directory account. This auditing can be done by the BCF SII, teacher, case managers, security staff, etc. Information about the auditing process is available through a shared BCF drive. The Assistant Director can be consulted for this document.
- In addition to these routine checks, random reviews of internet access (including website history and attempted access) should be done.
- All website audits should be documented, with any security breaches reported immediately to the BCF CAO, SII team, and the Department's Education Manager and IT Manager.

Email Monitoring

- Per the computer use agreement (Policy 24.10, Attachment B) that is signed by every student enrolled in education programming requiring a computer and/or internet access, computer use is not confidential. Each student signs off on the following statement:

    > *I understand that my computer use and/or internet access is not confidential and may be viewed or otherwise monitored by appropriate staff at any time.*

- The BCF teacher will keep an updated list of all student email IDs and passwords. This list will be shared with the SII team, and others, who will randomly check student email accounts for appropriate use.

Videoconferencing

- Students are allowed to attend remote programming through videoconferencing, if approved in their education plan, given the following:
  - The student provides the teacher with the who, what, when, where and why's of the videoconferencing session(s);
  - The teacher and BCF team approves the videoconferencing session(s);
  - The teacher, approved DOC staff or volunteer, sets up the Zoom session(s); and
  - The student signs the Videoconferencing Consent Form.

- The student should never send out a link for videoconferencing session(s).

Support

- DOC staff, OIT and outside vendors support the educational technology at BCF.
- Any issues (for example: whitelist support, system outages, AD questions, other support related to the BCF client hardware or software) should be directed to the BCF CAO, or designee. The BCF CAO, or designee will notify the Department's Education Manager and IT Manager, who will identify the appropriate support.

  - If services go out, the first step, after contacting the Department's Education and IT Manager, is to have BCF staff and the outside vendor double check client and server health.
    - Snow Pond Tech is the current outside vendor and can be contacted at support@snowpondtech.com
    - This service may result in a fee.

  - OIT can be consulted by contacting (207) 624-7700 and letting them know "the education network at Bolduc is not working properly, please have it assigned to network services for investigation." The BCF team does not need to call spectrum directly. OIT will check the network health and call spectrum to restore services if needed.

Process Auditing

- *Per Policy 24.10, Procedure F, a staff designated by the facility CAO must ensure that all computers used by clients are audited at least quarterly.* Documentation of the audit shall be forwarded to the Department's IT Manager, or designee.
- BCF staff will review education programming and the SOP for computer/internet use, supervision and monitoring at least quarterly and shall submit requests for changes in the SOP through the CAO, or designee, as well as the Department's Education Manager and IT Manager.

Documentation

- A logbook will be used to document computer and/or internet usage including, but not limited to, the following:
    o   Any outages or reported issues
    o   Any student concerns
    o   Monitoring and auditing
    o   Breaches or suspected breaches

Security Breaches

- If there are any security breaches, or suspected security breaches, staff shall follow Policy 24.10, Procedure G.

Staff Training

- The BCF teacher will create a PPT or video presentation for all staff to watch that provides an overview of the college program, the need and the process for internet usage, monitoring, browser reviewing, auditing processes, security protocols, etc.
- Staff training will be ongoing - to include new staff members, SOP updates, refresher training, etc.

SAMPLE TECHNOLOGY VENDORS FOR CORRECTIONAL EDUCATION

The following are examples of vendors that provide devices and other technical support for correctional education. Note that is not an exhaustive list nor does it represent endorsement.

Laptops

- ATLO Software
- World Possible

Tablets

- American Prison Data Systems
- Edovo
- JPay
- GTL

This page is left intentionally blank.