Idaho Department of Juvenile Corrections Administrative Policy/Procedure	NUMBER	REVISED	REVIEWED
	230	01/03/2025	01/03/2025
		EFFECTIVE	PAGES
		3/16/2000	8

SUBJECT: USE OF INFORMATION TECHNOLOGY

CATEGORY: FISCAL, IT, PURCHASING

Policy

The Office of Information Technology Services (ITS) is designated to oversee and execute the coordination and implementation of all information technology services and cybersecurity policies within the state of Idaho, pursuant to section 67-827, Idaho Code. The Idaho Technology Authority (ITA) was created within ITS pursuant to section 67-832, Idaho Code. Section 67-833, Idaho Code, sets forth the powers and duties of the ITA, which states in part that the ITA shall "…within the context of its strategic plans, establish statewide information strategic plans, establish statewide information technology and telecommunications policies, standards, guidelines, conventions and comprehensive risk assessment criteria that will assure uniformity and compatibility of such systems within state agencies".

The Idaho Department of Juvenile Corrections (IDJC) supports the ITA. The purpose of this policy is to establish standards for the appropriate use of computers, the Internet and e-mail within state agencies; bar state employees from using state resources to access the Internet or e-mail for the purpose of conducting political activity or for monetary gain; and reduce the risk of inappropriate or inefficient use of IDJC technological resources including, but not limited to, computers, Internet access and e-mail. As the use and accessibility of technology increases, so does the risk that the technology might be used inappropriately or inefficiently.

It is therefore the policy of the IDJC that all employees are expected to follow the procedures as noted in this policy. Accessing, transmitting, displaying, downloading, or storing any material or software deemed to be in violation of any federal, state, or local law or rule, or ITA, ITS, or IDJC policy is prohibited. Disregard for policies or other improper use of computers, Internet and/or e-mail may result in cancellation of an employee's access and/or disciplinary action, up to and including dismissal and/or legal action.

Operating Procedures

I. IDJC Information Technology (IT) Department responsibilities

A. Installation of all computer software, hardware, and approved peripherals.

B. Basic support of all standard software, hardware, and approved peripherals.

C. Ensure all software is licensed and has been obtained legally.

D. Ensure the IDJC is compliant with all ITA policies, standards, and guidelines.

II. State property, confidentiality, and security

A. Computer–For the purposes of this policy includes any computing device which accesses the IDJC network, i.e., smartphone, reader, laptop, tablet, etc.

B. Peripherals–For the purposes of this policy includes any non-computing device, i.e., a thumb drive, printer, scanner.

C. All work-related materials and information created, transmitted**,** stored, or deleted on the IDJC network or attached peripherals, may be accessed and/or restored by authorized personnel. All work-related files stored on these types of devices are the property of the state of Idaho and are subject to the terms and conditions of the Transparent and Ethical Government statute (Idaho Code 74-101 et seq.) (Formerly known as Idaho Public Records Act).

D. Computers, peripherals, e-mail, and access to the Internet are tools for meeting the business needs of the IDJC. **These tools are state property and their use is routinely monitored by the ITS and the IDJC.**

E. Peripherals (IDJC-owned or individually purchased) may contain confidential data or have access to confidential data, for example, the IDJC network and e-mail system. As such, in the event any of these items are lost or misplaced, the supervisor and IT staff must be immediately advised.

F. All computers that are synchronized with the IDJC network should be password protected.

G. Employees should not have any expectation of privacy as to the use of IDJC-purchased tools, including e-mail, or any agency data stored on any agency computer peripheral.

1. The Director, or designee, reserves the right to order the inspection of any computer or peripheral used to attach to the IDJC network.

2. If any files or e-mail being inspected have been encrypted, the employee shall provide the Director, or designee, with the password(s) or decryption keys necessary to decrypt this information. Failure to provide passwords or decryption keys shall result in disciplinary action, up to and including dismissal.

H. When computers or peripherals are shared between employees, any employee that is on **non-paid** time will yield the computer or peripheral to employees that are on **paid** work time. Employees may use IDJC's computers, with supervisor's approval, to complete homework assignments for IDJC sponsored/approved training and education during **non-paid** time.

I. Employees may use the Internet for non-business research or casual browsing **only during non-paid time.**

III. IDJC computers

A. Software and Program Updates

In order to maintain the efficiency of the network, IT routinely reformats IDJC computers and servers. Every effort is made to give advance notice to the employee when a computer requires reformatting.

B. Use of IDJC computers

1. All work documents are to be saved to a network folder or drive. This ensures recoverability of lost documents. Data stored on a local 'C' drive or removable storage devices are not backed up, and, therefore, not recoverable in the event of a hardware failure or when a computer is reformatted.

2. Employees who learn of unauthorized use of the IDJC network, unauthorized release of information, or unauthorized use, downloading or copying of computer software, must notify the appropriate supervisor, who in turn notifies the regional IT Support technician.

3. Employees may move their desks as needed. However, if the IDJC computer equipment needs to be unplugged to accommodate the move, please consult with IT.

C. IT Support

1. Send an e-mail to IT@idjc.idaho.gov regarding any non-emergency issue with an IDJC computer. For emergency issues, such as videoconferencing or e-mail, call the appropriate regional IT Support person. If a regional IT Support person is unavailable, contact another region.

2. Send an e-mail to support@IJOS.idaho.gov regarding an issue with IJOS (Idaho Juvenile Offender System).

3. Send an e-mail to spam.email@idjc.idaho.gov regarding any and all virus and hoax warnings. It is IT's responsibility to research warnings, prevent false alarms, and determine how to best protect the IDJC network.

D. Security and access

1. Passwords: Passwords are for individual employees and are not to be shared with others. Each employee is held responsible for unauthorized use of their network password.

2. If access to an absent staff member's computer files is needed, the staff member's supervisor contacts IT Support.

3. In the event a staff member requires access to certain folders on the IDJC DataCenter, the owner of the folder must give permission to IT Support to grant access.

4. For individually-assigned computers, employees should save all work and use the "locked computer" function when leaving a computer unattended. Individually assigned computers must be left powered on (but not logged on) so overnight updates may be performed. For employees working with a 'shared' computer, each employee must log off when not using the computer, or before exiting the room where the computer is located.

5. Juveniles are prohibited from accessing staff computers and the IDJC administrative network(s).

E. IDJC staff are responsible for closely supervising and prohibiting juveniles' access to sensitive, confidential, or inappropriate material available in IJOS, in the IDJC DataCenter, or by way of any computer-based source.

F. IDJC staff are responsible for prohibiting access to information for other juveniles, whether that information is stored in hard copy or electronically.

G. IDJC staff functioning as case managers may allow juveniles to view their own case information, whether that information is stored in hard copy or electronically, as determined necessary or advantageous to meet a treatment objective.

H. IDJC education staff functioning as part of a multi-disciplinary team may allow juveniles to view their own case information, whether that information is stored in hard copy or electronically, as determined necessary to develop student learning plans.

I. At the discretion of the teacher, juveniles, under close supervision, may use Smart Board-type technology in the classroom to complete education-related tasks.

IV. Electronic Messaging

A. Use of IDJC Electronic Messaging

1. Since state electronic messaging is provided to employees as a tool to aid in the performance of their job duties and responsibilities, it should not be used for any communication of a purely personal/private or nonbusiness nature during assigned work schedule.

2. **Inappropriate use of state electronic messaging includes, but is not limited to, personal letters, personal or other announcements or solicitations, and announcements of social events.** An occasional note to another person, similar to a telephone call, is acceptable.

3. It is an expectation of the IDJC that all communications sent by state electronic messaging will be professional, respectful, and model IDJC values.

4. State electronic mail should not be routinely sent to all agency e-mail users**.**

   Extreme care must be taken when using the "Reply to All" feature when communicating with more than 25 people since this can effectively decrease the productivity of the network and employees.

5. IDJC employees should have no expectation of privacy for any electronic messaging transmitted by or to them using state network resources. As such, an employee should determine whether electronic messaging is the proper medium by which to broadcast the information.

6. **State** electronic messages are **the property of the state of Idaho.** Electronic messages are subject to existing document retention and public records policies; may be discoverable evidence (documents requested by courts); and may be copied, saved, or seen by third parties, both internal and external to state government.

B. E-Mail support

1. If a questionable e-mail is received, contact an IT technician before opening any attachment, especially those with extensions of *.exe, *.inf, *.bat or *.vbs. Be aware that e-mail containing viruses can come from anyone, even a trusted sender.

2. If unnecessary or suspected spam e-mail is received and the employee does not want to receive messages from the sender, employees can use Mimecast to manage their spam setting and block the sender.

V. Internet use

A. IDJC staff are encouraged to use the Internet to:

1. Further the mission of IDJC,

2. Provide effective service to all customers,

3. Identify innovative and creative methods to use resources and improve services, and

4. Promote professional development. Users of the Internet are to comply with all appropriate laws, regulations, and generally accepted Internet etiquette.

B. Unblocking Legitimate Websites

1. The IDJC has in place software that routinely blocks certain websites based loosely on keywords. Some legitimate business sites may therefore be blocked automatically.

2. If an employee is notified that a legitimate website has been designated as inappropriate, the employee will notify their supervisor who will request from the Division Administrator or Superintendent that the website be made accessible.

3. Following the approval of the Division Administrator or Superintendent, an IT technician will then manually configure the monitoring software to allow access to the particular site.

C. The display of any kind of sexually-explicit image or document on any IDJC network, computer, or peripheral is a violation of the Harassment and Discrimination (307) policy and procedure. In addition, sexually-explicit material may not be archived, stored, distributed, edited, or recorded using the IDJC network or computing resources.

D. Sensitive IDJC information should only be accessed via the secure network, the web mail server, or a Virtual Private Network (VPN).

Sending sensitive IDJC data to an unsecured e-mail account (Yahoo, Gmail, HotMail, MSN, etc.) is approved only for the purposes of communicating with members of the juvenile's treatment team or IDJC stakeholders. Any other use of unsecured e-mail is strictly prohibited and may be a violation of the Confidentiality/Privacy (328) policy and procedure, and may result in disciplinary action, up to and including dismissal.

VI. IDJC social media accounts

A. Creating and removing IDJC branded/sponsored social media accounts requires Division Administrator, IT, and Director approval. Any domains or accounts created for IDJC purposes will be registered through IDJC's IT services.

1. Social media sites and pages will clearly identify the IDJC as the site/page owner/sponsor.

2. Purchasing of domain names will be done through IDJC's IT services and IDJC's IT services is the sole agent for ownership and maintenance of domains representing the IDJC.

B. An IDJC staff member will be designated as the moderator of any IDJC sponsored social media account(s) to ensure adherence to this policy.

C. IDJC staff are expected to follow the Ethics and Standards of Conduct (324) and other agency policies when using IDJC sponsored social media.

D. Employees should be aware that the IDJC may observe content and information made available by employees through IDJC sponsored social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to the agency, the state, its employees, or customers.

E. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.

F. Employees are not to publish, post, or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with their Division Administrator, Legal Services, or Human Resources.

G. Social media networks, blogs, and other types of online content sometimes generate press and media attention or legal questions. Employees should refer to the IDJC's Community and Public Relations (630) policy and procedure for guidance related to media inquiries.

H. If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of their supervisor, Division Administrator, Legal Services, or Human Resources.

I. Appropriate permission is required before referring to or posting images of current or former employees, members, vendors, or suppliers. Additionally, appropriate permission is required before using a third party's copyrights, copyrighted material, trademarks, service marks, or other intellectual property.

J. The IDJC's computer systems are to be used for business purposes only. When using the IDJC's computer systems, use of social media for business purposes may be allowed with Division Administrator approval. (e.g., Facebook, X (formerly known as Twitter), IDJC blogs, YouTube, LinkedIn, etc.).

VII. Network traffic monitoring

A. In order to provide an efficient computer network environment, the IDJC has a responsibility to monitor any and all aspects of its computer systems including, but not limited to, websites accessed, instant messaging systems, chat groups, news groups, materials downloaded or uploaded, and e-mail sent or received by IDJC personnel and the juveniles placed in IDJC facilities. **Such monitoring may occur at any time, without notice, and without the user's permission.**

B. If, in the course of the above inspection, the daily logs reveal what appears to be a prohibited site (i.e., sexually explicit, etc.) the IT technician will inform the Human Resource Officer (HRO), or designee. The technician will not share the information with anyone else and will not be involved further unless there is similar activity or unless directed by the HRO, or designee.

C. If any website is found to have a negative impact on network traffic, IT may block the site from IDJC access. If this occurs, the technician will notify the IT Infrastructure Engineer IV and the HRO, or designee, as to why the site was blocked.

VIII. Internet monitoring reports

A. When an employee is suspected of violating this policy or personal usage of IDJC computer equipment is impacting the employee's productivity, the employee's direct supervisor may request from the HRO, or designee, that an Internet Activity report be provided. This request should include the employee's name, normal work hours, and time period in question. A report will be generated and given to the HRO, or designee, within three business days.

B. Retention: Records collected by the monitoring logs will be retained for a period of time according to available storage capacity.

IX. Hardware, peripherals, and software requests

A. It is the responsibility of the IDJC to install standard software on all computers according to the ITA policy.

B. The IDJC IT Infrastructure Engineer IV will evaluate all proposed hardware, peripherals, and software acquisitions from a compatibility and maximum technological resource utilization perspective only. The requesting Division Administrator will determine the functional need and business purpose and consult with Fiscal Services for the proposed hardware or software.

C. Any requests for hardware, peripheral, or software, other than what is routinely provided by the IDJC as per ITA guidelines, must be requested of the supervisor, who would then advise the Division Administrator.

D. To acquire hardware, peripheral, or software, other than what is routinely provided by the IDJC, these steps must be followed:

1. The Division Administrator, supervisor, and employee schedule a meeting with the IT Infrastructure Engineer IV, or designee, to review functionality, business purpose, and maximum technological resource utilization.

2. If no IT problems are identified, the IT Infrastructure Engineer IV, or designee, provides written technical approval of the application to the requesting Division Administrator.

3. The requesting Division Administrator authorizes the appropriate IT technician to purchase the hardware, peripheral, or software, and the IT Infrastructure Engineer IV, or designee, installs the product.

4. If IT problems are identified, the IT Infrastructure Engineer IV, or designee, provides written explanation to the requesting Division Administrator as to why the request is not in the best technological interest of the IDJC.

X. Individually purchased computers and peripherals (Home PCs, Phones, Tablets, etc.)

A. IT will assist staff with IDJC connection credentials and basic connection setup only. The IDJC is not responsible for losses or damages incurred to computers or peripherals purchased by the individual due to power surges, viruses, computer failure, or any forces of nature. All upgrades, maintenance, additional software, and repair costs incurred are the responsibility of the employee.

B. In the event a computer or peripheral is lost or misplaced, employee should immediately advise the appropriate regional IT technician and their supervisor. Upon notifications, the employee must change their personal network password immediately. If unable to change the password, the employee will contact the appropriate regional IT technician for assistance.

XI. Exceptions to policy and procedure

Exceptions to any portion of this policy and procedure will be considered on a case-by-case basis with the approval of the Director. Written documentation of the Director's approval or denial will be sent to the Division Administrator, supervisor, employee, HRO, and IT Infrastructure Engineer IV.

XII. Policy distribution and acceptance

All employees, volunteers, contractors, and interns who have access to IDJC IT resources will sign the Use of Information Technology Employee Acknowledgement (DJC-055) form certifying that they have read, understand, and will comply with this policy. A copy will be given to all new employees as a part of the hiring process.

Reference: *Glossary of Terms and Acronyms*
Sections 67-832, 67-833, 67-827, 67-827A, Idaho Code
Section 74-101 Idaho Code
Idaho Technology Authority (ITA) policies, and associated standards and guidelines

Desk Manuals: *None*

Related Policies: *Harassment and Discrimination (307)*
Confidentiality/Privacy (328)
Community and Public Relations (630)

Related Forms: *Use of Information Technology Employee Acknowledgement (DJC-055)*
Non-Employee Computer Access Request (DJC-290)