

Division of Public Defender Services
Administrative Human Resources Policies & Procedures

<i>Policy # 608</i>	<i>USE OF COMPUTER EQUIPMENT AND MOBILE DEVICES</i>
<i>Effective</i>	<i>November 1, 2019</i>

POLICY

The Division of Public Defender Services provides computer equipment and mobile devices for the use by authorized employees to more efficiently conduct the official business of the Division. The Division of Public Defender Services reserves the right to establish and maintain conditions, rules and regulations regarding the use of computer equipment, mobile devices and access to State resources. For purposes of this policy the following definition are in place for clarification:

- A. Mobile Devices: Smart/Cell Phones, Laptops and Tablets
- B. Computer Equipment: Desktops, Printers, Fax, Network VPN Key, Scanners and Copiers

GENERAL INFORMATION

Computer equipment, mobile devices and related systems have been provided in order to assist Division employees in the efficient and effective discharge of their responsibilities in accomplishing the mission of the Division. Because of the size, scope and complexity of these systems, it is imperative that all employees adhere to certain rules and regulations. Primary among these regulations is the prohibition of improper, non-work related or unauthorized use of computer equipment, mobile devices and related systems.

GENERAL CONDITIONS AND REGULATIONS

Only employees, volunteers, contractors, and interns who have been granted use of computer equipment, mobile devices and related systems are permitted to use such equipment and systems. Usage of computer equipment, mobile devices and related systems must be in accordance with the employee's job duties and responsibilities.

Access to State, Judicial & Division systems will be determined by the employee's supervisor.

User passwords should not be shared except with the employee's supervisor or other authorized staff.

Information concerning security measures regarding the Division's computers, mobile devices and related equipment, and communications systems should not be disclosed without prior authority from appropriate management personnel.

Computer equipment, mobile devices and related systems are not to be used for personal gain or political activity.

Employees must not deliberately bypass or tamper with security measures designed to protect information and systems (example anti-virus software)

Personally assigned computer equipment and mobile devices shall be the responsibility of the assigned employee at all times. Lost, stolen and damaged equipment must be reported immediately to the employee's supervisor and to the following:

Division of Public Defender Services
Administrative Human Resources Policies & Procedures

Policy # 608	<i>USE OF COMPUTER EQUIPMENT AND MOBILE DEVICES</i>
Effective	<i>November 1, 2019</i>

Computer Equipment Systems Department 860-509-6409
Mobile Devices: Administrative Services Unit at 860-509-6435, lost or stolen devices should also contact 860-509-6471 or 6473 so Mobile Device can be shut off.

DESKTOP AND LAPTOP CONDITIONS AND REGULATIONS

In order to limit the Division's legal liability for the use of unlicensed software and to facilitate support, employees are not permitted to add or delete software programs or other applications without the expressed permission from the Systems Department.

The computer and mobile devices desktop/home screen contains the icons necessary to run the approved programs. Employees may place icons containing shortcuts from authorized software on Division computers.

Freeware/shareware is programming that is offered at no cost or nominal cost. Generally, it is the policy of the Division not to use freeware/shareware for normal business applications. Exceptions are made on a case-by-case basis with approval from the Systems Department. There should be no expectation of support for these applications.

Screen saver programs may not be downloaded from the Internet or installed from any other sources. There is potential for screen savers to conflict with Division standard software or operating system programs. The screen savers that are delivered as integral components of the operating system are the only ones that are approved for use.

Use of unlicensed software is prohibited.

INTERNET AND E-MAIL CONDITIONS AND REGULATIONS

Persons accessing the Internet using Division computers, mobile devices or network should have no expectation of privacy. Monitoring and recording of sites visited may be undertaken without specific notification according to Section 604 of this Manual.

Personal internet use is prohibited. List of examples: participating in the viewing or exchange of pornography or obscene, offensive materials; engaging in other illegal or inappropriate activities using the Internet; personal job searches; real estate searching; vacation planning; shopping on-line for non-work related items; paying bills; any activities for private, commercial purposes, such as business transactions between individuals and/or commercial organizations checking/viewing stocks or sports scores or conducting any personal financial planning activities; political activities, etc.

Sending or receiving personal email. Having personal email application (Gmail, Hotmail etc.) for the purpose of checking personal email. Forwarding jokes or pictures/videos; sending or forwarding messages referring to political causes or activities not related to the legislative

Division of Public Defender Services
Administrative Human Resources Policies & Procedures

<i>Policy # 608</i>	<i>USE OF COMPUTER EQUIPMENT AND MOBILE DEVICES</i>
<i>Effective</i>	<i>November 1, 2019</i>

business of the Division; messages concerning participation in sports pools, baby pools or other sorts of gambling activities; religious activities; stock quotes; vacations; distribution groups or “listservs” for non-work related purposes; solicitations or advertisements for non-work related purposes and any activities for private, commercial purposes, such as business transactions between individuals and/or commercial organizations.

Any activities where users engage in acts that are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, broadcasting unsolicited mailings or other messages, creating unnecessary output or printing, or creating unnecessary network traffic.

The displaying or transmitting of sexually explicit material, the transmission or use of e-mail that contains ethnic slurs, racial epithets, or anything else that may be construed as harassment or offensive to others based on their race, color, creed, marital status, national origin, ancestry, sexual orientation, mental retardation, mental or physical disability, including but not limited to blindness is strictly prohibited and could result in appropriate disciplinary action.

The downloading of software to a Division computer from the Internet is only permitted with the approval of the Systems Department. Any such unauthorized action is a violation of Division policy and is strictly prohibited.

The use of Internet radio, Internet video, streaming audio, or streaming video for personal use is prohibited.

The personal use of Division equipment to access the internet during non-work hours is prohibited.

The personal, non-business use of chat rooms is prohibited

The business use of Internet Relay Chat (IRC) must be pre-approved, as this functionality is normally prohibited by the Executive Branch’s Division of Information Technology.

SMART PHONES CONDITIONS AND REGULATIONS

Client, witness and all case related communication must be done using the Division issued cell phones/smart phone including for text, video, email communications and voice messages, phone calls, document or photo exchange. **Employees are not to use their personal accounts or cell phones/smart phones to communicate with clients or witnesses or maintain any case related information.**

Cell phone/smart phone shall be kept in the protective case and tempered glass shield provided. All repairs shall be administered through the Administrative Services Unit.

Upon termination or retirement the cell phone/smart phone with all assigned equipment shall be returned. The employee will be financially responsible for any items not returned.

Division of Public Defender Services
Administrative Human Resources Policies & Procedures

<i>Policy # 608</i>	<i>USE OF COMPUTER EQUIPMENT AND MOBILE DEVICES</i>
<i>Effective</i>	<i>November 1, 2019</i>

Employees whose job responsibilities include regular or occasional driving shall refrain from using their cell phone/smart phones while driving. Employees may utilize hands free or personal blue tooth cell phone/smart phones to make and receive phone calls. Reading or sending texts message while driving is strictly prohibited.

Employees charged with traffic violations resulting from the use of their cell phone/smart phone while driving will be solely responsible for all liabilities that result from such actions.

Employees are required to follow Division policy regarding recording, photographing or videotaping while using the assigned cell phone/smart phone.

Client and case information received via the Division issued cell phone/smart phone should be downloaded and saved electronically in Justware or printed and retained in the client file as soon as possible after receipt, except as required for ongoing operational needs. Client information (with exception of contact information) should not be maintained or archived on the Division issued cell phone/smart phone.

Personal use of a cell phone/smart phone for phone calls and texts is permitted on a limited basis. Excessive use of a cell phone/smart phone is prohibited and shall result in elimination of the privilege. Any roaming charges that may occur involving personal calls or texts will be reimbursed to the Division. In addition, employees may use the internet to access information concerning items such as school or daycare closing or weather related occurrences. Employees may set up alerts regarding this matter. Employees may provide the phone number as an emergency contact regarding children and/or other family members.

Employees with questions concerning the appropriate use of the Division's computer systems or mobile devices should consult with the Manager of the Information Services Unit or the Director of Human Resources.

ADDITIONAL RESOURCES

Public Act No. 98-142, An Act Requiring Notice to Employees of Electronic Monitoring by Employers, and the State of Connecticut's "Electronic Monitoring Notice"

[State of Connecticut Electronic Monitoring Notice](#)

State of Connecticut Acceptable Use of State Systems Policy (November 2006)

<https://portal.ct.gov/OPM/Root/Policies/Acceptable-Use-of-State-Systems-May-2006>

Division of Public Defender Services
Computer and Mobile Device Use

EMPLOYEE NAME:	DATE OF HIRE:
DATE TRAINING MUST BE COMPLETED BY:	

I have been provided with the Division of Public Defender Services policy on Computer and Mobile Device Use.

I have reviewed this policy and agree to follow it.

Employee

Date

Human Resources Staff

Date