Georgia Department of Public Safety
Policy Manual

SUBJECT **UTILIZATION OF TECHNOLOGIES**	POLICY NUMBER **14.01**
DISTRIBUTION **ALL EMPLOYEES**	REVISED DATE **8/3/2018**
	POLICY REVIEWED **8/3/2018**

14.01.1 Purpose

To establish the Department's policy in regard to the proper use of technology in the workplace, and to communicate to Department employees their responsibilities with respect to use of Department equipment and/or services.

14.01.2 Policy

The use of Department technologies is for business related usage and will be subject to limitations provided in this policy.

This policy applies to all employees of the Georgia Department of Public Safety, as well as any consultant or contractor doing business with the Georgia Department of Public Safety.

14.01.3 Definitions

For purposes of this policy, the term "technologies" means computer hardware, software, systems and services (including e-mail and Internet access, whether via Department issued, personally owned or any other devices), as well as other electronic forms of communication including, but not limited to, tablets, telephones (including cellular), pagers, fax machines, copiers, etc. owned or provided by the Department.

Since advances in technology continue to accelerate, each employee is expected to use sound judgment in determining what is, or is not, sufficiently related to the description provided here.

14.01.4 General Provisions

A. Any personal use of Department technologies should be incidental when compared to business related usage, and will be subject to limitations, as provided in this policy. Under no circumstances will any of the "prohibited uses," as outlined below, be justified as an incidental personal use of Department technologies. Any personal use of Department technologies would also be governed by other Department policies related to such usage (unlawful harassment, outside employment, etc.). The Department expressly reserves the right to access Department technologies, at any time and without prior notice to employees, in order to ensure compliance with the provisions of this policy. Department employees have no expectation of personal privacy with respect to Department technologies.

B. Department technologies are the property of the State of Georgia, Georgia Department of Public Safety. In addition, any message, document, or other product arising from the utilization of these technologies are, and shall remain, the property of the State of Georgia, Georgia Department of Public Safety. Because these items are the property of the State of Georgia, Georgia Department of Public Safety, they are not the property of any individual employee or user of Department technologies; nor are they to be considered to be the personal property of any such user.

C. The Department reserves, and intends to exercise, the right to review, audit, intercept, access, and disclose any and all messages, documents, or other products created, received, or sent over the electronic communications systems described in this policy. The content of any such message, document, or product may be disclosed without the consent of any individual, and without any prior notice to the individual.

D. The confidentiality of any message, document, or product should not be assumed. The use of passwords for security purposes does not create an expectation of privacy for any individual user; nor is any such expectation of privacy to be assumed.

E. The Department, like any employer, is subject to requests for production of documents attendant to legal proceedings. Moreover, since the Department is a public employer, it is subject to requests for documents under State open records laws. Messages, documents, and products arising from the utilization of technologies are subject to public scrutiny. All individual users are expected, as a matter of Department policy, to be aware of the potential for exposure arising from such scrutiny, and to govern their personal behavior in such a way to enhance the public's confidence in the Department.

F. The installation of any software or hardware on a Department technology without prior approval from their Division Director through the chain of command and from the Division Director responsible for the Technology Section is prohibited. The Chief Information Officer will maintain a file with all denials and approvals of request for software and hardware installations.

14.01.5 Prohibited Uses of Technologies

A. Department technologies may not be used to solicit, convey, or recruit for any commercial ventures, religious or political causes, or other outside organizations where the Department prior to dissemination has not approved such communication.

B. Department technologies are not to be used to create or send any offensive or disruptive messages, including but not limited to messages containing profanity, sexual references or innuendo, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, religious or political beliefs, national origin, or disability.

C. Department technologies are not to be used to search for, visit, or receive (download) any sites containing any written, pictorial, audio, or other depiction of information that might be considered offensive or disruptive in nature. Included in this category of sites would be sites containing material one may reasonably construe to be sexual in nature, or any other sites portraying information not reasonably considered to be of business use to the Department.

D. Department technologies are not to be used to condone or facilitate any of the above-prohibited activities. An individual user of Department owned technologies

who willfully receives prohibited information or materials, or one who engages in facilitating dissemination of such materials (forwarding files received from others, for example) will be equally in violation of this policy as one who engages in the initial creation of such prohibited information.

14.01.6 Reporting Requirement

All employees of the Department, including consultants or contractors doing work for the Department, are required, as a matter of policy, to immediately report any violations or alleged violations of this policy through their normal chain of command. Alleged violations of this policy shall be investigated thoroughly, and prompt corrective action shall be taken where deemed appropriate. It will be the responsibility of the Division Director responsible for the Technology Section to assist in any and all investigations of alleged violations of this policy on department technologies. No computer equipment will be seized or examined without the assistance of the Director responsible for the Technology Section.