INTERNAL POLICY & PROCEDURE

Topic Category:
Information Security and Use of Technology

Policy Title:
Acceptable Use Policy

Purpose:
Information Security's (InfoSec) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the Georgia Department of Education's (GaDOE) established culture of openness, trust and integrity. InfoSec is committed to protecting GaDOE, its staff members, and partners from illegal or damaging actions.

Effective security is a team effort involving the participation and support of every GaDOE Covered Person who deals with information and/or information systems.

Applicability:
This Policy applies to all Georgia Department of Education (GaDOE) or affiliated GaDOE staff members, consultants, contract workers and temporary staff ("Covered Persons") who access GaDOE systems (Technology based resources) and data.

All Covered Persons are required to read and sign the Acceptable Use Policy Acknowledgement of Compliance form found in Appendix A to this policy. The signed statement shall be placed in the Covered Person's personnel file if the Covered Person is an employee. If the Covered Person is a consultant, contract worker, or temporary staff, then the signed statement shall be kept by the Covered Person's supervisor.

Policy:

1. Use of GaDOE Systems and Devices

1.1. GaDOE Systems are to be used for GaDOE professional activities and personal use should be minimized.

1.2. Limited personal use of GaDOE Systems may be permitted with the following restrictions:

- The personal use does not interfere with job duties, responsibilities or performance. For Covered Persons compensated on an hourly rate basis, the use does not result in GaDOE paying the Covered Person wages for time spent on that personal use.
- All such usage shall be kept to a minimum and not incur any cost to the GaDOE, including the cost of paper or ink. .
- The personal use does not involve texting from any GaDOE Device where the text message results in a payment that will be charged to GaDOE as the account holder.
- The personal use does not interfere with other Covered Persons who are using GaDOE systems for appropriate business reasons or disrupt the intended use of GaDOE systems.

- The personal use does not constitute any form of employment or business activity other than for GaDOE.
- The personal use does not include access to gambling sites, pornographic sites or other inappropriate sites or materials.
- The personal use does not include political campaigning or unauthorized fund raising.
- Personal use should not expose GaDOE to unnecessary risks or violate applicable laws or other GaDOE Policies.

1.3. Covered Persons must adhere to the above restrictions whether in the office or offsite, including when using or accessing GaDOE systems remotely.

1.4. Covered Persons must not install any GaDOE prohibited software on GaDOE systems including personally owned software.

1.5. Connecting non-GaDOE Devices to any GaDOE System without prior approval from Information Security is prohibited. This includes connection to the GaDOE network either by wire or Wi-Fi connection.

1.6. Agency workers shall immediately report lost computing devices, communications devices, telephones, identification badges, or other devices used for identification and authentication purposes according to Agency incident reporting procedures. See the Computer Security Incident Response Policy for additional information.

1.7. GaDOE forbids user activities that could compromise the security of the infrastructure. No password guessing or cracking, vulnerability scanning, disruption of network services, or other general hacking activities are permitted.

2. Email, Instant Messaging & Cell Phone Use

2.1. Covered Persons must use their GaDOE email account to communicate GaDOE business matters on behalf of the Agency through email.

2.2. Covered Persons must not use public email systems such as Yahoo mail, Gmail, etc. to communicate GaDOE business matters.

2.3. Covered Persons must not forward business messages or other electronically-stored information from their GaDOE accounts to their personal accounts, except for messages related to their personal benefits (e.g., retirement, health, taxes, etc.) information.

2.4. Covered Persons must not use their GaDOE email address to register or create accounts on external websites (e.g., amazon.com, ebay.com, linkedin.com) for personal use.

2.5. Covered Persons must not use GaDOE Systems to create, store, send, or display chain letters or pornographic, defamatory, or maliciously false material or the like. This applies regardless of whether anyone is offended by or even knows about the material.

2.6. Covered Persons are responsible for ensuring the proper use of their GaDOE email account. Any actions performed with a Covered Person's account is the responsibility of the email account holder.

2.7. Covered Persons must use extreme caution when opening e-mail attachments or clicking on hyperlinks received from known or unknown senders. The attachments or hyperlinks may contain malware.

2.8. Covered Persons are prohibited from conducting GaDOE business via personal messaging or other means of written communications that are not archived by GaDOE for public records. This would include, but not be limited to, social media (i.e., Facebook, Twitter, etc.) or personal e-mail.

2.9. If a Covered Person receives a message related to Agency business via personal text messaging or personal email, the employee should immediately inform the sender of this policy and demand that future communications be sent via approved methods (e.g., the Covered Person's GaDOE email address or telephone number).

2.10. Covered Persons must not use a GaDOE-provided hand-held cell phone while operating a vehicle. This includes, but is not limited to, answering or making phone calls, engaging in phone conversations, and reading or responding to emails, instant messages, and text messages. If Covered Persons need to use phone, they must pull over safely to the side of the road or another safe location. In situations where job responsibilities include regular driving and acceptance of business calls, hands-free equipment may be used to facilitate the provisions of this policy. Under no circumstances are employees required to place themselves at risk or break the law to fulfill business needs. Covered Persons who are charged with traffic violations resulting from the use of their phone while driving will be responsible for all financial liabilities and associated penalties that result from such actions.

3. **Copyright Information**

3.1. Covered Persons must comply with applicable copyright laws and terms and conditions of license agreements for software and published material. In addition, Covered Persons must ensure that the software can be used without requiring the purchase of additional licenses. All purchases should follow the GaDOE Purchasing guidelines.

3.2. Covered Persons must not use GaDOE Systems to download, store, duplicate, distribute, print or use copyright material from any source (published works, the Internet, etc.) without the copyright owner's permission.

4. **Personally Identifiable Student Records**

4.1. Covered Persons who have access to personally-identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and other applicable laws and regulations, as they relate to the protection of the parents' and students' privacy concerning student information.

4.2. Covered Persons must follow GaDOE Reporting, Exchanging & Storing Personally Identifiable Information Standard Operating Policy.

4.3. Covered Persons shall not use access to student records information for personal gain. In no case shall personally-identifiable information be released publicly.

4.4. Covered Persons must refrain from viewing or printing personally-identifiable information except to perform their assigned duties.

4.5. Covered Persons authorized to access personally-identifiable information shall execute a separate acknowledgment indicating they are aware of additional provisions of applicable laws and regulations. The form shall be provided by and kept on file by the business unit that owns or oversees the information.

5. **Employee Data**
   - 5.1. Covered Persons are prohibited from disclosing confidential information accessed in the system or from using the information for personal purposes or personal gain.
   - 5.2. The "casual viewing" of employee data constitutes misuse of access, is not acceptable, and will not be tolerated.

6. **File Sharing and Data Storage**
   - 6.1. GaDOE uses pre-defined file sharing or storage services for conducting or communicating GaDOE business matters. Any non-standard service must be approved by Information Security before use.
   - 6.2. Covered Persons are responsible for making sure that their data is stored on network drives to ensure their data is backed up in a manner that the data can be recovered in the case of theft, loss, or system crash.
   - 6.3. Users shall not use free online (Cloud Computing) storage solutions to store GaDOE data. Only the agency provided storage resources should be used to store data.

7. **Internet and Network Usage**
   - 7.1. Only GaDOE-approved devices (both GaDOE-owned and Non-GaDOE) are permitted to connect to the GaDOE network.
   - 7.2. A guest network is provided for sponsored users in which Non-GaDOE-owned devices can connect to gain access to the Internet.
   - 7.3. Covered Persons must not connect GaDOE systems or Non-GaDOE Devices to the guest network.
   - 7.4. Covered Persons must not attach devices to GaDOE's network that provide wireless access or other shared network connections to the GaDOE network (such as wireless routers or cell phones used as wireless hotspots).
   - 7.5. Covered persons are not allowed to host personal websites on GaDOE Systems.
   - 7.6. GaDOE reserves the right to block access to Internet sites deemed inappropriate (e.g., sexually explicit sites, gambling-related sites, etc.) on all networks they manage.
   - 7.7. Covered Persons are not allowed to produce personal web pages or websites that appear to be official GaDOE web pages/websites.
   - 7.8. Covered Persons shall not run their laptops in wireless sharing or Hot Spot modes. This potentially allows other users to connect to the laptop in a peer-to-peer connection.

8. **Protecting Access to GaDOE Systems**
   - 8.1. GaDOE reserves the right to remotely manage and enforce security policies on all devices that connect to GaDOE Systems and to wipe all GaDOE-specific data on the devices at its discretion.
   - 8.2. Covered Persons must take appropriate actions to protect from loss or theft GaDOE-Devices and Non-GaDOE Devices used to access GaDOE systems.

8.3. Covered Persons must lock their screens when leaving their GaDOE Devices unattended for more than 10 minutes.
8.4. Covered Persons must not permit anyone who is not a Covered Person (e.g., family member, friend) to use their GaDOE Device or applications on their personal device used to access GaDOE Systems for any purpose.
8.5. Covered Persons must cooperate with Information Security-related activities such as helping to resolve security incidents.
8.6. Covered Persons shall not share their GaDOE accounts, personal identification numbers, identification badges, or other devices used for identification and authentication purposes.
8.7. Covered persons have the responsibility to promptly report the theft, loss or unauthorized disclosure of GaDOE information and assets including employee badges and agency provided encrypted key fobs.
8.8. Covered Persons shall immediately report suspected account compromises to their supervisor and to the GaDOE Information Security Manager.
8.9. Authorization for applying a power-on password (BIOS-enabled passwords) shall come from the Information Security Manager.

9. **Password Management and Authorization**
9.1. Covered Persons must keep passwords private, securely hidden and protected and must not share passwords with anyone unless they are authorized and authenticated for such access. This includes managers, support staff members, or Information Security Personnel.
9.2. Covered Persons must construct passwords to meet the following guidelines:
- Must contain at least 15 alphanumeric characters.
- Must contain both upper and lower case letters.
- Must contain at least one number (for example 0-9)
- Should contain at least one special character (e.g., !@#$%^&*<>?)
- Should not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- The strongest and easiest passwords to remember are passphrase passwords. For example, create a password based on a song title, or other phrase. For example, the phrase, “Until this very moment, this password was secure” could become the password UTVM, tpws1 or another variation.

10. **Covered Person**
10.1. Covered Persons must not use any feature on any GaDOE Device available in Web browsers that allows a system to remember user accounts and/or passwords.
10.2. Covered Persons must not circumvent any authentication or security mechanism, nor modify, bypass or disable the security configuration of their GaDOE Device.
10.3. Covered Persons should not access GaDOE data they are not expressly authorized to.

11. **Reviewing and Restricting the Use of GaDOE Systems**

11.1. Subject to limitations of local law, without prior notice and at any time, and only for legitimate business purposes (such as for investigations or information security monitoring or in the context of litigation or similar proceedings), GaDOE reserves the right to have authorized personnel access, monitor, record and inspect the use of GaDOE Systems connected to or used to access the Agency network or facilities, and all data and information located on such GaDOE Systems.

In addition to the foregoing, a Covered Person's use of GaDOE Systems constitutes the Covered Person's consent to this activity by GaDOE. Therefore, a Covered Person should have no expectation of privacy with regard to the use of GaDOE Systems. The Agency's right to access, monitor, record and inspect the use of GaDOE Systems extends to internal and external communication and to communication a Covered Person may deem "personal" (including communication and from personal email accounts, such as Gmail and Yahoo accounts) if accessed through GaDOE Systems.

11.2. Nothing within this Policy or within the policies referenced herein is intended to prohibit communication concerning wages, benefits, or other terms and conditions of employment, or that otherwise are legally protected under the National Labor Relations Act or any other applicable law.

12. **Termination of Employment**

12.1. Upon termination of their employment or work assignment at GaDOE, Covered Persons must return all GaDOE Devices, property, equipment and electronically stored information to the Agency in accordance with applicable Agency procedures.

Effective Date:
05/01/2017

Appendix A

Acceptable Use Policy Acknowledgement

I acknowledge that I have received and read the [GaDOE Acceptable Use Policy]. I understand and agree that my use of GaDOE Systems is conditioned upon my agreement to comply with the Policy and that my failure to comply with this Policy may result in disciplinary action, up to and including termination of my employment, civil liability, or other adverse action.

_____ _____

Signature of Employee Date

_____

Name of the Employee (Print)