

Descriptor Term:	Description Code	Issued Date:
	726—Fiscal Management (GDOE Employees)	June 30, 2014
	Rescinds:	Issued:

EDUCATION TECHNOLOGY USE POLICY

BOARD POLICY:

The primary purpose of the Guam Department of Education (GDOE, District) communication network is to support and enhance teaching and learning to prepare all students for success in lifelong learning.

All GDOE employees shall use the District’s technology (network, telecommunications, video, hardware, and software) in a responsible efficient, ethical and legal manner in accordance with the vision of the District, local and federal laws, regulations, and restrictions, Guam Education Board (GEB) policies, and other applicable mandates. The use of the District’s educational technology (not limited to Internet, telecommunications, hardware and software) is a privilege, which may be revoked for inappropriate behavior. Users are responsible for understanding the policy and guidelines as conditions for use. Educators and school personnel are accountable to teach and use technology responsibly.

GDOE’s Education Technology Policy shall include established rules and regulations for all users accessing the GDOE network. Use of the District’s technology that is inconsistent with this policy may result in the loss of access, legal action, and disciplinary action up to and including termination of employment.

Internet service shall be filtered and used in compliance with the Children’s Internet Protection Policy (CIPA) and other relevant regulations of the Federal Communications Commission. GDOE blocks or filters content over the Internet that the District considers inappropriate for students. This includes pornography, obscene material, and other material that may be harmful to students. GDOE may also block or filter other content deemed to be inappropriate, lacking educational related content, social media with inappropriate content, or that pose a threat to the GDOE network.

The Superintendent shall establish rules and regulations in adherence to this policy which must be included in the GDOE Personnel Rules and Regulations. In order to use the District’s technology, employees must sign the approved Educational Technology Standards of Operations and Technology User Agreement (form) contained in the Appendix. The User Agreement has incorporated the following guidelines:

I. ACCEPTABLE EDUCATIONAL TECHNOLOGY USE GUIDELINE

- A. Teachers and other school support instructional staff will be trained on and exposed to the appropriate use of the Internet, video, telecommunications and other educational technology with students, to monitor their use, and intervene if the resource is not being used appropriately.

- B. GDOE employees shall practice appropriate and safe online behavior, including interaction with other individuals on social networking websites, in chat rooms, and are prohibited from cyber bullying. School principals and division heads shall provide professional development to make employees aware of appropriate practices.
- C. GDOE employees must sign the Technology User Agreement form before they are allowed to access the GDOE network.
- D. The school principal, division head or worksite administrator is responsible for maintaining the signed Technology User Agreement forms for all employees at the respective school or work site. The signed form shall be available upon the request by the District.
- E. All devices accessing the GDOE network shall be subject to random monitoring. GDOE shall monitor users' online activities and reserves the right to access, review, copy, store, and/or delete any electronic communication or files.
- F. All use of the Internet must be in support of work, educational and research objectives consistent with the mission and objectives of GDOE.
- G. Proper codes of conduct in electronic communication must be used. Giving out personal information is inappropriate and therefore restricted. Extreme caution must always be taken in revealing any information of a personal nature.
- H. Network accounts are to be used only for its intended purpose and only by the authorized owner and user.
- I. All communications and information accessible via the network should not be assumed to be private property.
- J. The school principal or worksite administrator must approve creation of or subscription to blogs, wikis or other online communities. Prior administrative approval for such subscriptions is required for faculty and staff.
- K. Subscriptions will be monitored and maintained, and files will be deleted from the personal fileserver mail directories to avoid excessive use of fileserver hard-disk space.
- L. As a user of GDOE network/communications services, the user must be polite and exhibit exemplary behavior on the network or telephone.
- M. The Superintendent will periodically review and make determinations on whether specific uses of the network are consistent with the acceptable use and practice and report back to the GEB. This Policy will be reviewed and updated at least once every three years per GEBP # 120.3 as well as in conjunction with the District's technology plan in order to insure consistency.

II. UNACCEPTABLE USES OF GDOE TECHNOLOGY

- A. Transmitting (sending) any material in violation of any local or federal law (e.g., copyright materials).
- B. Using, posting or distributing profane, lewd, threatening, bullying, or abusive language in email messages, material posted on web pages or social media sites.
- C. Accessing, posting, or distributing harassing, discriminatory, inflammatory, or hateful material, or making damaging or false statement about others.
- D. Vandalizing equipment or software to include damaging computers and disrupting the operation of the network or telephone services.
- E. Using GDOE network services or telephones for personal financial gain,

- commercial activity or illegal activity.
- F. Giving out personal information about another person, including home addresses or personal phone numbers.
- G. Using the network for commercial advertisement or political lobbying.
- H. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users on the network.
- I. Using the network to disrupt the use of the network by others.
- J. Destroying, modifying, or abusing hardware and/or software.
- K. Maliciously using the network to develop programs that harass other users or infiltrating a computer or computing system and/or damaging software components of a computer or computing system.
- L. Sending hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors on the network.
- M. Installing unauthorized software, including shareware and freeware, for use on GDOE (school and administrative) computers.
- N. Using the network to access or process pornographic material, inappropriate text files or files dangerous to the integrity of the network.
- O. Using any website, application, or methods to bypass GDOE's network content filtering device.
- P. Downloading entertainment software/files (videos, music and non-instruction games) or other files not related to the mission and objectives of the Guam Department of Education.
- Q. Using for entertainment software/files (videos, music and non-instruction games) or other files not related to the mission and objectives of the Guam Department of Education.
- R. Gaming not approved by the school principal or worksite administrator.
- S. Establishing network or Internet connections to live communications, including voice and/or video (relay chat), without the authorization of the school principal, worksite administrator or the GDOE E-rate Compliance Officer.
- T. Other unacceptable use of the network.

III. GDOE WIRELESS NETWORK ACCESS

GDOE believes that providing network access for employees' personal electronic devices will enhance their educational and work experience by expanding access to the resources provided by the Internet. For this reason, GDOE has set up a wireless network. Prior to employees accessing the network, the signed Education Technology Acceptable Use and Wireless Network Use forms *must* be on file.

- A. *Acceptable Devices.* Employees may access the GDOE wireless network with any device with 802.11 connectivity. Employees may only access the network with devices that are their own personal property.
- B. *Content.* Filtered access to the Internet will be provided for employee owned devices as well as access to any district provided web-based applications that would normally be accessible to from home.

- C. *Personal Responsibility.* The District assumes no responsibility for the loss of, theft of, or damage to any personal device that an employee connects to the GDOE wireless network or any information on that device.
- D. *Security.* Employees shall not impair the security of the GDOE network. This expectation includes but is not limited to:
 - 1. Employees are expected to maintain up to date antivirus and antispyware protection on all devices that are connected to the GDOE wireless network. Devices without up to date security programs may be denied access to the network.
 - 2. Employees are expected to safeguard all network passwords. Employees should not share network passwords with others and should change passwords frequently. Employees are expected to notify their supervisor or an administrator immediately if they believe their account has been compromised.
 - 3. Employees are expected to log onto the GDOE wireless network only with their account and not to allow others to use their account or to use the accounts of others, with or without the account owner's authorization.
- E. *No Technical Support.* Employees are responsible for setting up and maintaining the devices that they connect to the network. The District will not provide technical support for employee owned devices.
- F. *Authorized Use.* Employees may use the GDOE wireless network during work hours for work related activities.
- G. *Inappropriate Use.* The GDOE network is a shared and limited resource and all users have an obligation to use that resource responsibly. Employees are provided access to the GDOE wireless network primarily for work purposes. Incidental personal use of the network is acceptable, but employees should not use the network for personal activities that consume significant network bandwidth or for activities that violate school or work policy or local law. These include but are not limited to:
 - 1. Online gaming (e.g., World of Warcraft) unless approved as a curricular resource.
 - 2. Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights. Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material.
 - 3. Conducting any activity that is in violation of school policy or local, state or federal law.
 - 4. Participating in political activities not sanctioned/approved by administrators.
 - 5. Conducting for-profit business.
 - 6. Using hacking tools on the network or intentionally introducing malicious code into the District's network.
 - 7. Using any software or proxy service to obscure either the employee's IP address or the sites that the employee visits.
 - 8. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.

9. Accessing or attempting to access material or systems on the network that the employee is not authorized to access.
- H. *No Expectation of Privacy.* The District can and GDOE will monitor Internet access and activity on the District's network, including but not limited to sites visited, content viewed and email sent and received. The District may examine an employee's personal device and search its contents if there is a reason to believe that school or work policies, regulations, or guidelines regarding access to the network or use of the device have been violated.
- I. *Disruptive Activity.* Employees should not intentionally interfere with the performance of the GDOE wireless network and the District's overall network.
- J. *Unauthorized Networks.* Employees may not create unauthorized wireless networks to access GDOE's wireless network. This includes establishing wireless access points, wireless routers and open networks on personal devices.
- K. *No Use of Wired Networks.* Employees may use only the GDOE wireless network for personal devices. They may attach personal devices to the GDOE wired network with prior approval of the Data Processing Manager.
- L. *Consequences of Inappropriate Use.* Employees who misuse GDOE's wireless network will be subject to discipline which may include loss of access to wireless or all Internet access and/or other appropriate disciplinary or legal action in accordance with the GDOE Personnel Rules and Regulations and applicable laws.

IV. EMAIL USE GUIDELINES

- A. The GDOE provides electronic mail to employees to enable them to communicate effectively and efficiently with other staff members, government officials, companies, and partner organizations.
- B. If you are in any doubt about an issue affecting the use of electronic mail, you should consult your school principal, division head, or worksite supervisor.
- C. Check electronic mail daily.
- D. Include an address line before sending a message.
- E. Include subject line in your message.
- F. Perform housekeeping duties by deleting electronic mail messages when they are no longer needed.
- G. Respect the legal protections to data and software provided by copyrights and licenses.

V. UNACCEPTABLE EMAIL USE GUIDELINES

- A. Printing electronic mail messages unless absolutely necessary.
- B. Forwarding electronic mail messages sent to you personally to others, particularly news groups or mailing lists, without the permission of the originator.
- C. Using electronic mail for personal purposes.
- D. Sending excessively large electronic mail messages or attachments without administrative approval.
- E. Sending unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to multiple people.

- F. Participating in chain mail or pyramid email or similar schemes.
- G. Representing one's self as another person.
- H. Using electronic mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive, or libelous.

VI. OTHER EDUCATIONAL AND TELECOMMUNICATIONS/NETWORK USE GUIDELINES

- A. All District users will abide with the intent of this policy.
- B. All users will be responsible to the school site or worksite administrator or appropriate designee for the purpose of this policy.
- C. All messages relating to or in support of illegal activities will be reported to the appropriate authorities.
- D. This policy is related to Board Policies on CIPA, 379, and 836.
- E. GDOE cannot be held accountable for the information that is retrieved via the network.
- F. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and will monitor messages.
- G. GDOE will not be responsible for any damages users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by user negligence, errors or omissions. Use of any information obtained is at the user's risk.
- H. GDOE makes no warranty/warranties with respect to:
 - 1. The content of any advice or information received by a user, or any costs or charges incurred as a result of seeing or accepting any information;
 - 2. Costs, liabilities, or damages caused by the way the user choose to use his or her access to the network.
 - 3. GDOE reserves the right to change its policies regulations and guidelines at any time.
- I. All email activity may be monitored.
- J. All email and external content may be scanned/monitored by the networks system administrator for offensive material.

**Adopted by the second Guam Education Policy Board 11-3-06.
Amended by the 6th Guam Education Board on 06-30-14.**



K. Erik Swanson, PhD
Superintendent

Upi Elementary School

Home of the Totots!

Phone: (671) 633-1382 • Email: upi@gdoe.net
Mail: 501 Mariner Avenue, Barrigada, GU 96913



Julie K. Salas, Principal
Mabel Uncangco, Assistant Principal

EDUCATION TECHNOLOGY USE POLICY USER AGREEMENT

I have read, understand, and will follow Guam Education Board Policy 726 Education Technology Use Policy when using computers and other electronic resources owned, leased, or operated by the Guam Department of Education. I further understand that any violation of the policy that is illegal, prohibited, immoral and/or unethical may result in disciplinary actions up to and including termination, revocation of access privileges, and/or appropriate legal action.

Print Employee's Name

Employee's Signature

Date



K. Erik Swanson, PhD
Superintendent

Upi Elementary School

Home of the Totots!

Phone: (671) 633-1382 • Email: upi@gdoe.net
Mail: 501 Mariner Avenue, Barrigada, GU 96913



Julie K. Salas, Principal
Mabel Uncangco, Assistant Principal

Faculty/Staff Agreement for the Acceptable Use of the Guam Department of Education’s Wireless Network for Faculty/Staff Owned Devices at Guam Department of Education (GDOE) Schools/Divisions

This agreement may only be executed by Faculty/Staff who have previously returned an “Employee Acceptable Use” form signed allowing them to use the Internet at school. This agreement provides additional authorization to access the GDOE wireless network using personal devices. It does not supersede any information in the “Staff/Faculty Handbook” or GDOE Personnel Rules and Regulations. GDOE believes that providing network access employee’s personal electronic devices will enhance the work and educational experience by expanding employees’ access to the resources provided by the Internet. For this reason, GDOE has set up a wireless network.

- A. **Acceptable Devices.** Faculty/Staff may access the GDOE wireless network with any device with 802.11 connectivity. Faculty/Staff may only access the network with devices that are their own personal property.
- B. **Content.** Filtered access to the Internet will be provided for Faculty/Staff owned devices as well as access to any district provided web-based applications that would normally be accessible to faculty/staff from home.
- C. **Personal Responsibility.** The district assumes no responsibility for the loss of, theft of or damage to any personal device that a faculty/staff member connects to the staff wireless network or any information on that device.
- D. **Security.** Faculty/staff shall not impair the security of the GDOE network. This expectation includes but is not limited to:
 - 1. Faculty/Staff are expected to maintain up to date antivirus and antispyware protection on all devices that are connected to the GDOE wireless network. Devices without up to date security programs may be denied access to the network.
 - 2. Faculty/Staff are expected to safeguard all network passwords. Faculty/Staff should not share network passwords with others and should change passwords frequently. Faculty/Staff are expected to notify an administrator immediately if they believe their personal account has been compromised.
 - 3. Faculty/Staff are expected to log onto the staff wireless network only with their account and not to allow others to use their account or to use the accounts of others, with our without the account owner’s authorization.
- E. **No Technical Support.** Faculty/Staff are responsible for setting up and maintaining the devices that they connect to the network. The District will not provide technical support for employee owned devices.
- F. **Authorized Use.** Faculty/Staff may use the GDOE wireless network unless otherwise informed by the network administrator or school administrator.
- G. **Inappropriate Use.** The GDOE network is a shared and limited resource and all users have an obligation to use that resource responsibly. Faculty/Staff are provided access to the GDOE wireless network primarily for educational or work purposes. Incidental personal use of the network is acceptable, but faculty/staff should not use the network for personal activities that consume significant network bandwidth or for activities that violate school policy or local law. These include but are not limited to:
 - 1. Online gaming (e.g., World of Warcraft) unless approved and used as a curricular resource.

2. Downloading software, music, movies or other content in violation of licensing requirements, copyright or other intellectual property rights. Downloading, viewing or sharing inappropriate content, including pornographic, defamatory or otherwise offensive material.
 3. Conducting any activity that is in violation of school policy or local, state or federal law.
 4. Participating in political activities.
 5. Conducting for-profit business.
 6. Using hacking tools on the network or intentionally introducing malicious code into the District's network.
 7. Using any software or proxy service to obscure either the employees' IP address or the sites that the employee visits.
 8. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or other security measures.
 9. Accessing or attempting to access material or systems on the network that the employee is not authorized to access.
- H. **No Expectation of Privacy.** The District can and does monitor internet access and activity on the District's network, including but not limited to sites visited, content viewed and email sent and received. The District may examine an employee's personal device and search its contents if there is a reason to believe that GDOE policies, regulations, or guidelines regarding access to the network or use of the device have been violated.
- I. **Disruptive Activity.** Faculty/Staff should not intentionally interfere with the performance of the GDOE wireless network and the District's overall network.
- J. **Unauthorized Networks.** Faculty/Staff may not create unauthorized wireless networks to access GDOE's wireless network. This includes establishing wireless access points, wireless routers and open networks on personal devices.
- K. **No Use of Wired Networks.** Faculty/Staff may use only the GDOE wireless network for personal devices. They may attach personal devices to the GDOE wired network upon prior approval of Data Processing Manager.
- L. **Consequences of Inappropriate Use.** Faculty/Staff who misuse GDOE's staff wireless network will be subject to discipline which may include loss of access to GDOE wireless network or all internet access and/or other appropriate disciplinary or legal action in accordance with the GDOE Personnel Rules and Regulations and applicable laws.

Faculty/Staff Name (Please Print)

Date

Faculty/Staff Signature