Intern Conduct Guidelines

Policy

Each intern participating in the State of Connecticut Legislative Internship Program will engage in appropriate and ethical conduct while performing official duties and while engaged in off duty activities that may directly reflect upon the General Assembly.

Standards of Conduct

Each State of Connecticut Legislative Internship Program intern will:

- Comply with all federal and state laws, regulations, and/or statutes, legislative policy and lawful instructions or directives.
- Ensure that a safe, secure and sanitary work environment is maintained.
- Report for work dressed in an appropriate manner. The "Standards of Dress," as defined in the Connecticut General Assembly Employee Handbook Sec. 8.4, (will be distributed at Orientation).
- Report to a supervisor as required when leaving the work site during work hours.
- Report any arrest and subsequent disposition, including conviction or loss of driver's license, to a supervisor *on the next scheduled workday following the arrest and disposition*.
- Inform the supervisor in writing of any change of address and/or telephone number in a timely manner.
- Report to the Program Director any medical condition or any medication being taken which could place the program participant or others at risk during the performance of a job duty. This information will be shared with the Capitol Police to be referenced in the case of an emergency.
- Act in a professional manner by showing respect to the public, other program participants, legislators, legislative aides, committee clerks, and other staff members.
- Maintain good stewardship of all state property and equipment.
- Maintain appropriate demeanor.
- Cooperate fully and truthfully in any inquiry or investigation conducted by the General Assembly or any law enforcement or regulatory agency.

The following are strictly prohibited:

- Acting in any way that jeopardizes the integrity of the General Assembly or the health, safety, or welfare of the public and/or staff.
- Removing state property from the Legislative Office Building without authorization.
- Using state resources, including property, equipment, or consumable supplies, for private benefit or gain.
- Reporting to work in possession of and/or under the influence of alcohol, recreational marijuana or illicit drugs.
- Entering a restricted work location unless on duty or otherwise authorized.
- Engaging in abusive, threatening or intimidating behavior or using obscene language.
- Engaging in sexual harassment and/or unlawful discrimination of any kind.
- Accessing or disclosing confidential information without authorization.
- Failing to report an accident or providing a false report.
- Engaging in any conduct or activity that constitutes or has the appearance of a conflict of interest.
- Appropriating or using any property belonging to the General Assembly, including computer equipment, without authorization and/or for inappropriate purposes.

Legislative Internship Dress Code

All attire must be appropriate for a business environment; for example, the attire must be clean, pressed, fit properly, and not show undue wear. Religious or cultural attire central to one's personal faith is permitted. Employees may wear clothing in accordance with their gender identity or expression.

Business Professional Attire
• For women, business professional attire consists of suits (with either pants or skirts), blazers (or blazer-alternatives) and dress pants or skirts, dress shirts (e.g., blouses, collared shirts, or knit tops), dresses, sweaters, and accessories that project a professional and neat appearance. Business professional footwear for women includes loafers, flats, heels, open-toed shoes, and dress boots.

• For men, business professional attire consists of suits, blazers, dress pants, dress shirts, ties, sweaters, and accessories that project a professional and neat appearance. Shirts should be tucked in and socks are required. Business professional footwear for men include loafers, dress shoes, and dress boots.

Intern Information Technology Guidelines

Each intern will be granted a legislative email account by the Director. Access to legislative computer systems personal computers (PCs) shall be restricted to those with a legitimate need for legislative data and shall be at the discretion of assigned legislators and/or office staff. Questions concerning access shall be directed to the intern's Supervisor, or the Director.

Prohibitions on Use
Interns may not use State PCs, portable computers, software, and supplies:

(a) for any business other than official legislative business;

(b) to access general bulletin boards or subscribe to non-business related list services;

(c) to play games, unless they are related to job training;

(d) to download unauthorized software or files, particularly interactive graphic files and executable (.exe) files; or

(e) to download, view, disseminate, or produce pornographic, sexually explicit, racially offensive, or other offensive material.

Interns shall not use State equipment for any purpose that is not authorized by policy of the Joint Committee on Legislative Management or in a way that could compromise the security of the legislative computer systems or the integrity of legislative data. Violators are subject to disciplinary action up to and including dismissal from the internship program.

Protection of Passwords, User IDs and Data
Access to systems requires an ID and a password. Passwords shall be kept confidential and interns are responsible for anything done that is attributable to their ID. If an intern's ID or password has been compromised, the Office of Information Technology Services shall be notified immediately. Interns shall not share access codes, passwords, access procedures, or system telephone numbers with anyone.

Interns who use a PC, or portable computer, are responsible for the equipment, the software loaded on the equipment, and the data stored in their accounts. Data stored in the intern's account shall be for legislative business only. Random checks of storage may be performed. Any theft or unlawful activity shall be reported to the intern's Supervisor, the Director, and the State Capitol Police immediately.

Interns are responsible for protecting the data on their PCs. Access to data should be limited to persons with a legitimate business need for the information. Data on a PC should be backed up on the users M:\ drive, not on the local drive (C:\) of the device.

Restrictions on Copying of Software

It is a violation of copyright laws, license agreements, and this policy to:

(a) make or use unauthorized copies of any licensed software,
(b) duplicate or use unauthorized copies of licensed software,
(c) have more than one copy of a licensed software package running, or
(d) load software on a PC, remove the disk and then use it to load another machine without proper license agreements.

Any questions about software licensing shall be directed to the Office of Information Technology Services.

PC Virus Protection

Each user is responsible for:

(a) using only approved software purchased by the Office of Legislative Management;
(b) scanning for PC viruses on a regular basis;
(c) scanning for viruses all files from any outside source prior to use

Interns shall report any suspected viruses to the Office of Information Technology Services immediately.

Internet Access and Use

The Internet is used both to access Internet sites and to exchange E-mail with persons outside the General Assembly. Internet access and services shall be used only for work-related activities. Communications sent or received through the Internet may be read or intercepted by anyone who is connected to the Internet. Consequently, confidential information shall not be sent via the Internet.

Internet activities on all computers may be monitored for misuse, visits to inappropriate web sites, and work unrelated to the requirements of the General Assembly.

Interns shall not use the Internet for the following purposes:

(a) transmission of, intentional receipt of, or viewing obscene, scandalous, illegal, offensive, or otherwise inappropriate information or other matter;

(b) transmission of confidential information;

(c) subscribing to contests or other sales-related “events”;

(d) subscribing to any commercial service without the authorization of the office director, unless the site is owned by a legitimate commercial enterprise and there is specific notice that the site does not make the E-mail addresses of its subscribers known to other commercial entities;

(e) downloading or receiving any executable (.exe) file; or

(f) any other use prohibited this Handbook.

If an intern receives prohibited information, the intern shall notify their Supervisor and/or the Director immediately.

Electronic Mail (E-mail)

E-mail is provided to interns for work-related uses. Interns shall not send personal messages using the General

Assembly's E-mail system.

The General Assembly reserves the right to monitor intern E-mail use and messages. Monitoring can be accomplished despite the assignment to individual interns of passwords for system security. The computer system's security procedures, message delete function, and an intern's personal password can be bypassed for monitoring purposes. Therefore, interns do not have any expectation of personal privacy in their use of the E-mail system.

An intern shall not send E-mail to all employees without approval of the intern's office director. An intern shall use good judgment when sending E-mail to a large number of recipients, being aware that E-mail is not without costs to operate and to store messages. Information that concerns employee activities shall be sent to the Office of Legislative Management for inclusion in *The Assembly Line on-Line*.

The following uses of the General Assembly's E-mail system are specifically prohibited:

(a) Sending any form of slanderous, harassing, threatening, or intimidating message, at any time, to any person. (Such communication may also be a crime, pursuant to sections 53a-182b and 53a-183 of the general statutes, and other laws.)

(b) Sending any message that discloses confidential information.
(c) Sending any copyrighted material, or other legally protected material. (This may also constitute a violation of law or contract.)
(d) Sending messages that constitute an impropriety or the appearance of an impropriety, or that are unprofessional or would embarrass the Legislative Department.
(e) Sending any other message that is prohibited by law.

If a particular behavior or activity is prohibited by the policies in this Handbook generally, it is also prohibited using the E-mail system. For example, interns may not use E-mail for solicitation purposes.

SPAM and MALWARE

Email scams and phishing attempts evolve constantly, hoping to take advantage of the latest trends and current events. Although the e-mails change, the people behind them inadvertently send up the same warning signs again and again. Please review the following tips to protect you and your computer:

1. No legitimate organization will ask for your social security, bank account or PIN number via e-mail.

2. Watch for typos or spelling mistakes**.**

3. Don't trust links to Web sites in e-mails from an email address you do not know.
   Never fill out a survey or enter a contest – requiring you to give personal information or "log on" to your account.

4. Got a "hot stock tip" via e-mail? SCAM, delete it.

5. Don't open an attachment from someone you don't know – even if it appears to be your bank or credit card company.

6. Some legitimate looking "e-mails" are actually just images, by clicking on the image you may install spyware.

7. Some scammers like to pose as technical- or customer support from a company you associate with – but fail to keep up with current events.

8. If you see the phrases "verify your account," "you have won the lottery" or "if you don't respond within XX hours, your account will be closed," it's a scam – every time. Hit the delete button and don't look back.

9. While you can't trust every e-mail that knows your name, you can definitely ignore the ones that start "Dear member" or "Hello friend." If your bank or credit card company is writing you, it knows who you are. So do your friends.

If you have to ask is this spam or phishing it probably is…….. Please report the message using the Report the message feature in outlook

The Connecticut General Assembly has mechanisms for managing spam and phishing attempts conducted via email. ITS continues to work on reducing the volume of nuisance email delivered to CGA inboxes. In support of this work, there are actions you can take to protect yourself, including a feature for Microsoft 365 to report messages.

Determining if an email is considered spam or phish.

The first step in knowing how to handle spam and phishing emails is to understand which type of message you have received.

- **Spam is unsolicited nuisance email.**
  - These usually appear as commercial messages sent to many recipients.
  - These can also include any unwanted content.
  - **Discard spam using the methods described further in this article.**

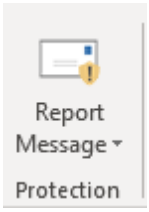
- **Phishing messages try to collect information.**
  - These typically try to convince you to provide protected information, such as a password, or other non-public / sensitive information.
  - These often include links and/or attachments.
  - Phish messages often appear to be sent from ITS, senior leaders, or other groups with authority.
  - **Please report phishing messages using the methods described further in this article.**

Reporting spam email

CGA manages spam using automated detection tools in the email service. Individuals may also use methods offered through the email system (Microsoft 365) to further manage spam on a personal level.

Microsoft 365 Email

1. Open the message you'd like to report as spam, so that it appears in a new window.
2. In the Outlook Ribbon (toolbar), ensure the **Message** tab is selected.
3. Select the **Report Message** button and choose **Junk**.



Following the steps will:

- Immediately move the message to your Junk folder.
- Adds the sender to your Blocked Addresses list, preventing the sender from emailing you again.
- Reports the message to our vendor, Microsoft, to improve their spam management Artificial Intelligence (AI), a tool the vendor uses to improve identification of these types of messages in the future.

- Contribute to the spam reputation (score for tracking of complaints for sending spam) of the sender with various email reputation services. Higher spam reputation scores result in service providers blocking more mail from that sender.
- For more information about managing your Block and Allow Senders lists in o365, see: Microsoft 365 Email: Blocking or allowing a sender.

Reporting Phish

Individuals should actively report phish messages. Reporting phish allows ITS to block the sender from emailing other individuals, blocks any malicious links within the email, and reports the message to our vendors to help improve their phishing detection mechanisms.

Microsoft 365 Email

1. Open the message you'd like to report as phish, so that it appears in a new window.
2. In the Outlook Ribbon (toolbar), ensure the **Message** tab is selected.
3. Select the **Report Message** option and choose **Phish**.

Sexual Harassment Prevention Training

All interns are required to attend the Connecticut General Assembly Sexual Harassment Prevention (SHP) training. The CGA Sexual Harassment Policy is explained in this training. No previous state trainings will substitute for the CGA SHP training without approval from the CGA Human Resources Director or team members.

Sexual Harassment Prevention training is mandatory and is assigned to each intern based on their work schedule. The scheduled training is considered part of work hours and takes place during scheduled work hours. If you are unable to attend the CGA SHP training due to an absence on the day of training, you must contact the Internship Director to schedule a CGA approved substitute training.

The CGA Sexual Harassment Prevention Policy can be found here for your reference. Additional references are below. If you need to report an incident of sexual harassment you can contact the CGA Internship program director, your caucus liaison, or the CGA human resources staff.

CGA Employee Handbook http://cgalites/olm/docs/Handbook.pdf

State Code of Ethics https://portal.ct.gov/ethics