2011
TECHNOLOGY USAGE POLICY
Objective

The foundation's Technology Usage Policy is designed to support the following goals:

- Support our people in doing their best work.
- Protect the foundation, including its information assets, reputation, and relationships with grantees and partners.

The foundation asks users to be informed and to use their best judgment when using technology resources. Inappropriate use of technology or failure to comply with this policy may result in disciplinary action for the user, up to and including termination of employment.

TABLE OF CONTENTS

1. Introduction ................................................................. 3
2. Information Security ...................................................... 3
3. Stewardship .................................................................. 5
4. Legal ........................................................................... 6
1. Introduction

1.1 Philosophy on Technology Usage

The Technology Usage Policy covers all technology used by foundation users in performing their jobs including, for example, personal computers, mobile phones, online services, and hotel kiosks. It does not attempt to cover all situations or answer every question regarding technology usage. Rather, we trust our users to use common sense and informed best judgment in making decisions in the best interest of the foundation. This policy contains information and guidelines intended to enable you to use technology to maximize productivity and effectiveness while also protecting the foundation, its reputation, and its information assets.

Protecting our information assets in today’s increasingly connected world is more important than ever, particularly with the rise of “hacktivism”—attacking an organization based on ideological principles. Groups whose ideology opposes the work of the foundation and its grantees may use hacktivist methodologies in an attempt to disrupt or cause harm to the foundation’s systems, networks, data, or reputation. The news is full of such examples that include attacks against foundation-funded organizations and initiatives. Because these attacks are based on ideology, a hacktivist organization often believes furthering its cause at all costs is a moral imperative.

The foundation maintains an active information security program to ensure that reasonable safeguards are in place to protect the foundation and its information. However, our philosophy is to balance information security with stewardship of resources and flexibility of technology usage. This means that every person working on behalf of the foundation has a responsibility toward securing information assets.

You are empowered to use technology to maximize your productivity with few restrictions. In return, your obligation is to make informed and educated decisions regarding the technology that you use so as not to expose the foundation to undue risk. If you encounter a situation that is not addressed or if you simply have questions regarding this policy, please contact the foundation’s IT Service Desk or Information Security.

2. Information Security

2.1. Foundation-issued Equipment

Foundation-issued equipment is for staff (that is, foundation employees and contingent workers) use only. Depending on your role at the foundation, you will be assigned foundation-issued equipment to use in performing your job. You are responsible both for the equipment issued to you and its use. Always exercise caution if leaving your equipment unattended.

2.2. User Credentials

Depending on your role at the foundation, you will be assigned credentials that grant you the access necessary to do your job. These credentials are for your use only, and you are responsible for their safekeeping. Your credentials provide access to your confidential personal information, such as HR data, as well as confidential foundation data. For these reasons, you must never share your password with anyone. Also, do not reuse your foundation passwords on external web sites or applications. If the external site is compromised, the foundation could be at unnecessary risk. Please contact the IT Service Desk immediately if you believe your credentials may have been compromised. Refer to the Password Management Guideline for best practices on creating and managing secure passwords.
2.3 Computer Safeguards
Foundation-issued equipment has been configured with a number of safeguards to assist you in having a secure computing experience. These safety mechanisms may include, but are not limited to, antivirus software, screen locks, firewalls, automatic software patching, and encryption. It is essential for the security of the foundation that these safety mechanisms remain enabled and functional as configured. Contact the IT Service Desk as soon as possible if one of these safeguards is not functioning properly.

2.4 Appropriate Storage Locations
Any information that could cause significant financial or reputational harm should be stored only in an approved manner on appropriate foundation-issued equipment and systems. The foundation has designated internal network storage locations (such as network drives, SharePoint, Unison, ICS, and Exchange), as well as approved externally administered systems (such as AP Master, Concur, BrassRing, and Workday) as appropriate storage locations for foundation data. Hard drives, outside of approved network storage, and other media (such as laptop or external hard drives, USB flash drives, and CD/DVDs) are not appropriate storage locations for foundation data beyond occasional and very short-term use. These devices are typically not enabled with the same safeguards as foundation-issued devices and may be easily lost or compromised.

You are responsible for complying with the foundation’s Records Management program and ensuring that foundation information is appropriately protected. More information about the storage and retention of foundation data may be found in the Records Management Policy and the Email Management Standards. The foundation is under no obligation to maintain, retain, back up, or return any data located on a temporary storage device (such as laptop or external hard drives, USB flash drives, or CD/DVDs). Any data stored on laptop hard drives may be removed at the foundation’s sole discretion and without prior notification.

In no event may any user delete or destroy data that may be relevant to a pending or threatened claim or government investigation. For more information, refer to the Records Management Policy, sections 1.1 Legal Hold and 1.2 Legal Release.

2.5 Information Management
As with the technology devices themselves, you are expected to use informed good judgment when handling foundation information. Exercise care when sending or receiving confidential information outside of the foundation. Email and online sharing services (such as YouSendIt and Dropbox) may not be sufficiently secure depending on the sensitivity of the information. When sending information outside of the foundation, please adhere to the Records Management Policy and use appropriate storage locations. (See section 2.4.)

2.6 Non-Foundation Devices
Generally, you are expected to use foundation-issued equipment for conducting foundation business. Do not connect non-foundation devices (that is, devices not provided and managed by foundation IT) to the foundation’s internal network. This helps ensure the safety and security of the foundation’s network and information assets.

You may access select foundation systems and data from non-foundation devices through specific external access services provided by IT. These services, along with applicable policies, standards, and guidelines, may be found in the Non-Foundation Device Services section of the IT Portal on The Commons. If you access these services, you must adhere to the service-specific terms of use.
2.7 Awareness of Surroundings
In order to prevent the inadvertent disclosure of confidential or sensitive information, consider your surroundings when you engage in discussions or work on sensitive documents. Be particularly careful in airports, airplanes, restaurants, and other public venues. Note that rooms containing camera or audio equipment may not be secure. Where available, in-room controls may be used to ensure cameras or audio equipment are disabled when not required.

2.8 Monitoring of Electronic Content, Electronic Communications, and System Use
It is not the foundation’s regular practice to monitor electronic content, electronic communications, or system use. However, the foundation reserves the right to perform such monitoring as it deems necessary. Monitoring may be performed without notification to support activities such as, but not limited to, operational maintenance, auditing, and security.

3. Stewardship
Stewardship at the foundation applies not only to money, but to the use and security of technology and information. In keeping with the foundation’s Guiding Principles, you are expected to consider stewardship in your decisions regarding technology and information resources.

3.1 Personal Use of Foundation Technology Resources
The foundation recognizes the importance of allowing occasional and limited personal use of foundation technology. In the case of certain classes of devices (such as mobile phones), alternate guidance may be provided regarding personal use. You are ultimately responsible for any and all activity that originates from your use of foundation technology. The foundation takes no steps to maintain, retain, back up, or return personal data. As foundation systems are subject to monitoring (see Section 2.8), you should not store sensitive or confidential personal information on foundation resources. Such permitted personal use does not include individual political activities, which should occur during off-duty hours, at the employee’s expense and without use of the foundation’s name, resources, facilities, or equipment. More information about these prohibited political activities may be found in the Conflict of Interest Policy.

3.2 Physical Loss
When transporting foundation-owned equipment, please be aware of your surroundings. Although the foundation has taken steps to prevent data from being misappropriated or misused in the event of lost or stolen equipment, you should treat foundation-issued equipment as if it were your own. The foundation does not back up data stored on mobile equipment. If you believe any of your foundation-issued equipment has been lost or stolen, contact the IT Service Desk immediately.

3.3 Software and Technology Services Not Provided by IT
The freedom to install software and use external technology services is a significant privilege and therefore carries significant responsibility. Unpatched software is a common source of viruses, worms, and other malware, which pose a threat to the foundation’s information assets. Software written by untrustworthy authors can result in loss of confidential data or system compromise. Use of online services can result in unintended disclosure of foundation information assets.

If you install software on a foundation-issued device or use external technology services, you must understand the associated risks (such as the trustworthiness of the author, download source, impact to information security, and system performance and reliability). You are responsible for managing these risks, including ensuring that the software or service is properly licensed (see Section 4.1) and kept current with security patches. If the software has an auto-update function, consider enabling it. Procurement of software and technology services must be in accordance with the foundation’s Travel and Expense Policy.
If you have any doubts or concerns, contact the IT Service Desk for advice, or do not install the software. For Windows and other officially supported applications (such as Adobe Reader and Java), foundation IT will provide regular security updates.

4. Legal

You are expected to use technology resources in accordance with all applicable laws and foundation policies.

4.1 Licensing and Copyright Laws

When installing or using software not provided by the foundation, you must ensure that the software is properly licensed. This also applies to copyrighted materials including music, pictures, videos, and movie files, as well as written media. Contact the Legal Department with questions about copyrighted material and the IT Service Desk with questions about software licensing.

4.2 Electronic Content and Messaging

You are encouraged to use electronic messaging technologies to facilitate the exchange of information and promote collaboration at the foundation. However, you may not send, download, store, or forward electronic messages or other electronic content that contain offensive language, images, sound clips, or harassing statements. This includes but is not limited to disparagement of others or inappropriate content based on race, sex, sexual orientation, religion, caste, creed, national origin, age, disability, marital or veteran status, or any other protected status. Please refer to the foundation’s Online Social Media Policy for additional information about online communication.

4.3 Recording of Video, Web, or Telephone Conferences

Before recording any meeting or telephone conference, organizers should determine whether recording the meeting session is appropriate. Further, to comply with privacy law, the organizer must inform all presenters and participants that the recording is taking place prior to the start of the meeting by providing the following announcement:

IMPORTANT NOTICE: This meeting is being recorded by the foundation. Any documents and other materials exchanged or viewed during the meeting session may also be recorded. By joining the meeting, you consent to such recording. If you do not consent to the recording, you have the option not to participate in the meeting.