TEMPORARY CHANGE REQUEST

TCR NO. P-088,R2-TCR-001

The Temporary Change Request (TCR) Form is to be used to process urgent or minor changes for PPPL Policies, Organization/Mission Statements and Procedures. The TCR should be used when changes are:
1) urgent, and can not wait the 2-4 week period for Department Head review/comment, or
2) minor, and do not warrant Department Head review.

Person Requesting Change: Jim Graham **Phone Ext: 2701**

Department Name: Best Practices and Outreach

Document Number: P-088 **Revision No.: Rev. 2**

Document Title: Computer Use and Use of Social Media

Reason for change:

Based on a suggestion from the Princeton University attorney, Policy P-088 is being renamed from "Computer Use Policy" to "Computer Use and Use of Social Media".

The intent is to ensure the policy is viewed as comprehensive; including the important social media content.

In addition, a few minor updates are being made to the referenced documents.

Change description: (Summarize and attach changed pages, with changes clearly indicated)

Change title from "Computer Use Policy" to "Computer Use and Use of Social Media".

Update references under References Section and under item #6.

1. Does this TCR significantly alter the intent or scope of the document? **YES:** **NO: X**

2. Does this TCR significantly impact **ES&H**? **YES:** **NO: X**

If 1 or 2 is **YES**, Explain why the changes should not be routed for Department Head review:

Bill Davis **10/14/14**
Department/Division Head Approval **Date**

John DeLooper **10/14/14**
Head, Best Practices and Outreach/designee **Date**

Release/Effective date of this TCR: **10/14/14**

Incorporate this TCR into next revision of this document? **YES: X** **NO:**

Subject:	Effective Date:	Initiated by:
Computer Use and Use of Social Media	6/22/12	Bill Davis Head, Information Technology and CIO
	Supersedes: *Revision 1, dated 8/18/8 and TCR-001*	**Approved:** Stewart Prager Director

TCR-P-088,R2-001

APPLICABILITY

This policy applies to all users of PPPL information and PPPL owned electronic assets. Electronic assets include computer hardware and software, network elements, and communication devices such as cellular phones, pagers and portable electronic devices.

REFERENCES

This policy is consistent with and augments the following documents: TCR-P-088,R2-001

- DOE Order 203.1 Limited Personal Use Of Government Office Equipment Including Information Technology
- DOE Order 580.1A Department of Energy Personal Property Management Program
- P-098 Use of Laboratory (DOE) Resources
- P-099 Limited Personal Use of Laboratory (DOE) Office Equipment, Including Information Technology
- Personnel Practices Manual: Usage of the University Name and Laboratory Resources

INTRODUCTION

PPPL electronic assets are funded by the United States Government to allow the staff to conduct the official business of the Laboratory. Official business includes all authorized work connected with the operation and maintenance of the Laboratory, its authorized research, development, educational and technology transfer programs, and associated administrative and support activities.

I. COMPUTER USE POLICY

Electronic assets and information created, stored, sent or received through PPPL electronic assets are the property of PPPL.

Users are expected to be responsible, considerate and ethical in using PPPL. See sections on "Reasonable Use of Computers" and "Examples of Inappropriate Activities".

Circumvention of the security features of PPPL electronic assets, including but not limited to probing, hacking, launching viruses and the wrongful use of passwords is prohibited. Users also may not use PPPL systems to "snoop" or access the email or other communications or information of others.

Least User Privilege

It is the policy of the Laboratory that all users of PPPL information systems adhere to the principle of Least User Privilege which means giving a user only those privileges which are essential to do his/her work. When applied to a computer use account the principle refers to the concept that all users at all times should run with as few privileges as possible, and also launch applications with as few

privileges as possible. The majority of daily business related computer operations do not require administrator (privileged) account access because few individuals need to install or update applications every day.

Hackers have the ability to compromise systems, making these systems participants in illicit activities, and/or making them vulnerable to harvesting of institutional data or intellectual property. Application of the Least User Privilege principle reduces security risk by requiring that all users, even those who have been granted administrator privileges, login with user privileges only, to make it more difficult for others to take control of their computers.

User Responsibilities:

- User Accounts and Assigned Systems: All users agree to maintain the integrity of their accounts and assigned systems and not to allow unauthorized individuals (including family members) access to them. Precautions include, but are not restricted to:
  - Keeping passwords secret and secure
  - Keeping electronic assets secure from unauthorized access and usage
  - Setting passwords for all applications and systems that provide the capability.
  - Using password-enabled screen saver. This security lockout feature shall automatically initiate after a maximum of 15 minutes of inactivity. The user must then reenter their password to gain access to the computer.
    - Domain and System Administrators should configure their lock out setting to a maximum of 10 minutes.
- Users may not access PPPL systems using another user's password or ID or disguise their identities while using PPPL systems.
- Software Protection: Users are responsible for complying with copyright, licensing, trademark protection and fair use restrictions.
- Virus Protection: Anti-virus software and safe practices must be used to prevent documents or email received from inside or outside PPPL from introducing viruses to personal computers or PPPL's network. Anti-virus software is intended to detect and prevent the introduction of viruses into PPPL's systems and must not be disabled or circumvented. Users are responsible for assuring that virus protection is in use and maintained up-to-date.
- When using non-PPPL equipment or networks to access PPPL electronic assets or information, users are responsible for ensuring that anti-virus programs are in use, and up to date.
- Passwords: Users must adhere to the PPPL password policy.
- Banners: Users must assure that the DOE warning banner is and remains installed on all systems for which they are responsible and for which it is feasible, and users must agree to adhere to the banner guidelines.
- Reporting violations: Users must report suspicious activity or known violations of this policy to a Designated Individual, indicated below.

Reasonable Use of Computers:

Minor incidental personal use of computing resources by staff members for purposes unrelated to work assignments is allowed, on personal time, if such use is consistent with the following:

- Does not involve illegal activities.
- Does not interfere with legitimate job activities or job performance.
- Does not result in greater than minimal cost to PPPL.
- Does not compromise security in any way.
- Does not involve activities that could potentially embarrass PPPL.

- Does not involve activities for the purpose of generating personal income, such as operation of an active business or working in part-time or consulting position for compensation. (Management of passive personal finances is acceptable).
- Does not involve any lobbying activities or any partisan political activities.
- Does not create the impression that the employee is acting in his/her capacity as a PPPL employee.

Examples of Acceptable non-work related activities:
The following are examples of minor incidental personal use of computer systems that are acceptable and adhere to the criteria above. Questions about appropriateness of intended use should be directed to a Designated Individual.

- Education, self-training and professional development.
- Personal correspondence or development of resumes.
- Personal research such as reading newspaper articles, checking airline prices, browsing sales catalogues, comparing prices, obtaining road maps, checking weather forecasts or road conditions.
- Acquisition of personal items such as airline tickets, or catalogue items.
- Managing personal finances, such as banking, paying bills, checking or managing retirement accounts, or preparing personal income taxes.
- Other appropriate internet access.

Examples of Inappropriate activities
The following are some examples of inappropriate use of PPPL resources that is prohibited. This list in not complete. Please contact a Designated Individual if you have a question about proposed usage.

- Supporting or accessing sites promoting hate language, harassments or threats.
- Supporting or accessing sites that ridicule others on the basis of race, creed, religion, sex, disability, nationality or sexual orientation.
- Accessing explicit sexually orientated material (e.g., pornography).
- Gambling.
- Operating a business or supporting for-profit organizations for compensation.
- Endorsing any product.
- Participating in any partisan or lobbying activities.
- Hosting services for purposes not related to PPPL business.
- Creating or forwarding chain letters or mass mailing not in connection with PPPL business.
- Violating licenses, copyrights or other computer related contracts
- Copying, distributing or otherwise using materials or information that may be protected by copyright or using such copyrighted information in a way that violates the copyright laws.
- Downloading or use of illegal or bootlegged software, movies or music (e.g. via “peer-to-peer” software).
- Using “hacker” software, password crackers or sniffers, without authorization.
- Downloading or opening large file attachments such as music or graphic files for personal use.

II. USING SOCIAL MEDIA AT PPPL

Definition:

"Social Media" is an umbrella term that encompasses the various activities that integrate technology, social interaction, and content creation. Social media uses many technologies and forms, such as blogs, wikis, photo and video sharing, podcasts, social networking, mashups, and virtual worlds.

Introduction:

Social media, such as Facebook and Twitter, is a powerful and emerging communications medium. Social media platforms are being embraced by the U.S. Department of Energy's Princeton Plasma Physics Laboratory (PPPL) as a key thrust of a strategic communications policy designed to maintain, build and expand the excellent research reputation of the Laboratory and develop a natural public constituency for its support and continued success. It is clear that PPPL can, through the use of social media, explore opportunities among its staff and members of the public to both encourage active participation within the Laboratory and foster connection to the public. As its cardinal trait is interactivity, social media will also allow PPPL to reach and engage new audiences.

Social media offers many opportunities to function as a positive communications platform for PPPL. It can convey key messages that will provide staff and other users with a sense of community and build increased public awareness of its programs and value to the nation and the world. It can provide information to previously underserved audiences and build new audiences by providing increased access to staff voices. It can serve as an important forum for conversations about a range of issues. Specifically, it can help reach diverse audiences including: prospective and current students to its graduate programs; graduate alumni; faculty; staff; funding agencies; policy makers; and other critical thinkers, including members of the mainstream news media. In the increasingly noisy environment of the public media landscape, the value of social media to the Laboratory in terms of maintaining and strengthening staff morale and providing a better understanding of plasma and fusion science to the public is great.

Policy for Use of Social Media:

1. Know and follow PPPL's Standards of Ethics and Conduct in the PPPL Personnel Practices Manual. As a representative of the Princeton Plasma Physics Laboratory, you are expected to respect the Laboratory's good name in your electronic dealings with those both within and outside the Laboratory.
2. When you compose, send, or redistribute electronic mail or voice mail, when you create or publish postings to World Wide Web pages (including images, blogs, social network sites, Twitter, or chat rooms), or mailing lists, or produce and submit broadcast video materials, consider whether you would make identical statements face to face with the person or people who may read, hear or view your work.
3. You are personally responsible for the content you publish on blogs, wikis or any other form of user-generated media. Be mindful that what you publish will be public for a long time and because of the distributed nature of Web indexing, may be difficult to expunge.
4. Using Laboratory technologies or access to the network provided by the Laboratory under its name, or in any other venue in which you are acting as an agent of the Laboratory, do not publish in any form anything that is malicious, harassing or libelous.
5. Comply with copyright, fair use and financial disclosure laws. Never post sensitive information such as export control data or personally identifiable information (PII). Social media is not

appropriate for the collection or storing of sensitive information such as personally identifiable information or export control information.

6. Ensure your use of social media tools complies with existing Laboratory policies including P-098, *Use of Laboratory (DOE) Resources;* and P-099, *Limited Personal Use of Laboratory (DOE) Office Equipment, Including Information Technology.* **TCR-P-088,R2-001**

DESIGNATED INDIVIDUALS:

Questions and concerns regarding this policy should be directed to the Chief Information Officer.

WAIVER OF PRIVACY RIGHTS:

The User expressly waives any right of privacy in anything they create, store, send or receive while using PPPL computer systems and Internet access.

MONITORING OF COMPUTER AND INTERNET ACTIVITIES:

PPPL has the right to monitor and log any and all aspects of its computer systems including, but not limited to, monitoring Internet sites visited, chat and newsgroups, file downloads and e-mail sent and received.

BLOCKING SITES WITH INAPPROPRIATE CONTENT:

PPPL has the right to utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit or any other material deemed inappropriate in the workplace.

PPPL ACKNOWLEDGEMENT:

On occasion an individual may receive unsolicited e-mail or inadvertently access a site that is deemed inappropriate under this policy. The individual will not be held accountable under these circumstances. If the unintended activity becomes prevalent the individual should report the incident to Helpdesk@PPPL.GOV.

ACKNOWLEDGEMENT OF UNDERSTANDING:

All users must accept the "Acknowledgement of Understanding" agreeing to comply with PPPL's Computer Use Policy before an account is created and activated. Reaffirmation of the commitment is required through the Cyber Security training for all users and the Letter of Integrity for employees. A violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.