GBLS TECHNOLOGY USE POLICY

INTRODUCTION

Greater Boston Legal Services is committed to providing quality equipment and services to the GBLS staff as they strive to meet the needs of our clients.

The goal of this document is to clarify the Information and Communication Technology ("ICT") policy of GBLS, the role and responsibilities of the Information Technology Team, and the responsibilities of the User in order to:

1. Comply with applicable laws, funder requirements, and GBLS policies.
2. Ensure a quality and efficient work environment.
3. Minimize user frustration.
4. Ensure a secure working environment to minimize the disruption of ICT services for our users and our clients' protection.
5. Enhance the IT Teams ability to provide ICT as economically and reliably as possible.
6. Provide GBLS staff with reasonable and efficient means to communicate with others, subject to existing GBLS policies.

By effectively communicating the details of this policy and our adherence to its measures we hope to better meet the needs of our clients by creating a secure and stable technology system.

DEFINITIONS

1. "GBLS" means Greater Boston Legal Services the legal services program at which the user is employed.
2. "ICT" means the Information and Communication Technology systems of GBLS and its branch offices. ICT includes items such as laptop and desktop computers, servers, networks, telephones, thumb drives or other portable storage devices, Internet service, printers, software, websites, and other hardware, software, or other electronic services used for the creation, dissemination or retrieval of information.
3. "User" refers to the person who is authorized to work with GBLS Information and Communication Technology systems and carries related responsibilities.
4. "IT Team," "Director of Technology," "Network Administrator," "Network Support Technician" refer to the people at GBLS with responsibility for computer maintenance and support.
5. "DD" means the GBLS Deputy Director, or acting director or one or more designees.
6. "DHR" means the GBLS Director of Human Resources or one or more designees.

GENERAL

Unauthorized use of GBLS computers and computer accessories is a violation of GBLS policy and grounds for discipline, including possible termination of employment subject to any applicable collective bargaining agreement. This policy applies to all GBLS computer users, including employees, contractors, volunteers and AmeriCorps volunteers.

OWNERSHIP AND CONTROL

All electronic machinery, including stand-alone and networked computer systems and all software including email and internet access to websites by GBLS computer users is the sole and exclusive property of GBLS. While we do not intend to regularly inspect email or internet history without cause there should be no expectation of privacy by any user of GBLS electronic equipment - including, but not limited to, email. GBLS reserves the right to monitor communication and data at any time, with or without notice, to ensure that GBLS property is not being used unlawfully or in violation of GBLS policy.

Any product including websites, emails, and documents of any sort produced by the use of GBLS technology is the sole and exclusive property of GBLS and not of the employee or user involved. GBLS reserves the right to access, review, record, and edit any and all such material. Such material can be used by GBLS without reservation for any purpose including, but not limited to, establishment of liability and employee discipline/termination subject to any applicable collective bargaining agreement.

All equipment and materials described above are provided primarily for the business purposes of GBLS and not the personal use of employees or other users. Occasional personal use is permitted within the other rules established by this policy. GBLS reserves the right to further limit/regulate such non-business uses subject to any applicable collective bargaining agreement. Any significant non-business use must be approved by the Deputy Director (DD) or the Director of Human Resources.

COMPUTER USE:

1. Duty of Care

Each user has a duty to treat GBLS computer equipment with respect and care. Please do not eat over your computer and keep the screen, keyboard, mouse and other parts clean from dust and debris. In the event of an accident, please notify the IT Department immediately so that potential damage may be minimized.

2. Conservation of Resources

GBLS permits the occasional personal use of GBLS ICT resources if the use does not (i) interfere with the user's work performance; (ii) interfere with any other user's work performance; or (iii) have an undue impact on the operation of GBLS's networks or equipment. Users must not use ICT for personal use in a manner that wastes ICT resources or unfairly monopolizes resources to the exclusion of other users. These acts include but are not limited to the sending of mass mailings or chain letters; subscribing to non-business-related e-mail list distribution services (i.e. Listserv's, mailing lists); spending excessive time on the Internet on non work-related activities; playing games; engaging in online "chat groups"; printing large

numbers of copies of documents that are not work-related; or otherwise creating unnecessary network traffic. Violations may result in discipline as stated above subject to any applicable collective bargaining agreement.

Users need to be aware that many commercial websites can redirect you to other sites, which may not be benign. Websites can place software on your computer without your knowledge - such software may, in the best case only slow down your computer and, in the worst case, infect your computer and the network with malicious software which may compromise the security of our network.

Because audio, video, and picture files require significant storage space and/or network bandwidth to send and receive, users should not download or stream these files unless they are business-related and even if business-related, users should be prudent in their bandwidth and storage consumption. Do not stream videos or music as background while you work. These activities use up our internet capacity. They cost GBLS extra money to maintain and overuse slows down the internet for everyone. **If staff cannot comply on a voluntary basis, we will have to restrict access to these activities as many employers already do.**

Accessing sites relating to pornography, sexual offerings, or gambling is also prohibited. One-time accidental access is excused; however, any repeated access is prohibited. **Accessing pornography or sexual offerings sites is a violation of GBLS policy and grounds for discipline, including possible termination of employment subject to any applicable collective bargaining agreement. See also the GBLS policy on Offensive Materials, http://www.gbls.org/staff/policies/personnel/offensive.htm**

3. Exclusive Use of Accounts

Users are to access their accounts and logins exclusively. Users shall not share their account or login information with anyone else. DHR may assign user accounts and login information or may request that Users provide their user accounts or login information for management purposes. No other disclosure is to be made or requested. Users should be aware that hackers might pose as ICT professionals to gain User login and account information.

4. Responsible Transmission, Viewing and Storage of Content

Except to the extent that it is necessary in the furtherance of specific work-related activity, material that is fraudulent, harassing, sexually explicit, profane, obscene, defamatory, discriminatory, or otherwise unlawful or inappropriate is prohibited from GBLS ICT. Unless work-related, such material may not be intentionally obtained, viewed, loaded, stored on, or sent by GBLS ICT. Users encountering or receiving this kind of material from another GBLS employee, intern, or volunteer, should immediately report the incident to the Director of Human Resources.

5. Public Access Computers

Offices may establish public access computers for clients and other visitors. The IT Team will set up these computers so that they do not have access to internal data resources and are only to be used in a manner consistent with how users may use GBLS ICT for non-work related purposes.

6. Limiting unwanted e-mail messages (SPAM)

Except for work-related purposes, users should not use their work e-mail addresses on commercial websites (e.g. Amazon, eBay) or use their work e-mail address for any commercial distribution lists as it will likely increase the level of unwanted e-mail.

7. Assignment and Use of Equipment Off-Site

GBLS authorizes users to take certain equipment off-site for work related purposes. Users are responsible for maintaining the security of the equipment against theft, damage or any otherwise prohibited use, such as operation by non-users. Users are responsible for checking with technical support staff to make sure that off-site use of ICT equipment does not compromise security of the information on the equipment or security of the greater GBLS network on the return of the equipment to the office. Should any off-site equipment be lost, stolen or damaged, the User must report it to the Director of Technology immediately.

Laptops, thumb drives or other portable storage devices are inherently insecure. Laptops should only be used to remotely access the network if a non-portable computer is not available. GBLS recognizes that some employees may use a laptop as their primary personal computer and may need to rely on that computer for remote access from home and when traveling. Confidential client matters should not be stored on such devices unless absolutely necessary. All GBLS property is equipped with encryption tools for transferring client confidential information. Please contact the helpdesk for assistance. If work documents are stored on a portable device, that information should be copied to the GBLS network as soon as feasible, and then the information on the portable device should be erased. Users should not place personal documents or information on portable devices as those devices may be re-formatted (wiped clean of any information) by the GBLS at regular intervals without notice. Restriction of Installation, Deleting and Copying of Software

Without prior authorization from the IT staff, users may not (i) copy software for use on their home computers or for distribution to a third party; (ii) install software on any GBLS computer or electronic device; (iii) download any software from the Internet or other online service to any GBLS computer or electronic device; or (iv) modify, delete, transform, recast, or adapt any software. However, the IT staff does permit upgrading of some programs. If users get a message requesting upgrade from a program such as Adobe Reader, it will likely have been approved by the IT staff and may be done, but users should seek confirmation from IT staff if they have any question. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to the Director of Human Resources.

INTERNET USAGE

No staff person should use GBLS equipment for purposes prohibited by law or GBLS policies. Users should keep in mind that Internet use is traceable. The burden of responsibility is on the User to inquire as to acceptable and unacceptable uses prior to use. GBLS will provide and publish frequently asked questions submitted by the unions or individual employees providing guidance on unacceptable uses of the internet including what significant non-business uses require approval and proper use of equipment off-site

Internet access at any computer owned/operated by GBLS is intended to be used exclusively in accordance with this policy.

Services available to users include Skype for voice and video conferencing, Web-Ex for on-line webinars, and downloading PDF files.

Services not available to users include downloading Exe or DLL files.

Please contact the IT staff for assistance with any of these services.

DISASTER RECOVERY

Users should be aware that the **network resources are backed-up daily**. Individual computers are **not backed up** by the IT Team. Therefore all GBLS related work should be saved on the network drive. **In other words, Users should not save work on their "C" drive. The "C" drive is not backed up.** Users may choose to make additional backups, but should seek training to assure that they're making the best backup choice and are in compliance with GBLS policies.

EMAIL USE

No email may be sent which violates federal or state law, including but not limited to, communications reasonably interpreted as discriminatory, harassing or in violation of regulations/policies of GBLS. The email system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability. Limited personal use of the email system is allowed unless it is excessive in the discretion of GBLS management or otherwise violates the provisions of this policy. Any extensive or prolonged personal use of email must be authorized by the Director of Human Resources.

Users are encouraged to avoid sending excessive email. Be considerate of the intended GBLS recipients of any email. Users should think twice before hitting the "reply all" key, and consider before sending any email whether it is appropriate/necessary to send it to an entire group (e.g. a unit, the program, etc) rather than one or more designated individuals. **Unnecessary email not only distracts from our client work, but also takes time to delete and clogs up individual email accounts.**

INSTANT MESSAGING

Instant messaging programs (IM) are not secure and provide easy entry for viruses or other malicious software to the GBLS network. Therefore IM should not be used from GBLS computers. If you need to use IM for business purposes please contact the IT staff.

SYSTEM PROTECTION

Intentionally launching any computer "worm," computer virus or other rogue program is prohibited by any GBLS computer user or anyone else assisted by any GBLS computer user. Any presence of system threats such as computer "worms," computer viruses or other rogue programs (including suspicious emails or attachments) must be reported immediately to the Network Administrator for protective and remedial measures. The Deputy Director shall be informed of any such occurrences by the IT department.

Computer viruses may be transmitted via emails with innocent appearing attachments. Such emails may appear to be sent by a friend or co-worker. **No unanticipated email attachment should be opened without first checking with the sender to verify its authenticity.** When sending an email with an attachment Users should "sign" the email by typing their name (first name is sufficient if appropriate) at the end of the email message. Using your name as a salutation at the end of the email message is an easy way for the recipient to tell if a message was sent by a person versus by a spammer (spammers just grab your email address and don't necessarily end the email with a name - or else they use a generic name like "The GBLS technical support group") **If in doubt about any email, do not open it. Contact the network administrator immediately**.

PUBLICATION OF FREQUENTLY ASKED QUESTIONS

GBLS will provide and publish frequently asked questions providing guidance on activities that may violate this policy including proper use of e-mail, non-business use that requires approval, use of the internet and proper use of equipment off-site.

VIOLATIONS:

Subject to any applicable collective bargaining agreement, any intentional and willful violations of the policies described above may subject the User to discipline, including, but not limited to termination of employment, or in some cases, legal action.

Summary of Personal Responsibilities Under

MA Personal Information Security Regulation 201 CMR 17

Beginning March 1, 2010, Massachusetts 201 CMR 17.00 which implements M.G.L. c. 93H requires all businesses to comply with standards designed to protect Massachusetts residents' Personal Information. As an employee of GBLS, you are responsible for following all procedures and practices regarding the protection of Personal Information, and participating in incident management, risk assessments, work processes, and control mechanisms that support the policy. Below are your individual responsibilities under 201 CMR 17.

Personal Information is defined as: a Massachusetts resident's first name and last name or first initial and last name, *in combination with* any one or more of the following data elements:

- Social security number;
- Drivers license number or state-issued identification card; or
- Financial account number, or credit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account.

Personal Information does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Security Awareness Training
All Employees are required to attend and complete mandatory security awareness training provided by GBLS within 30 days of your start date at GBLS.

Access to Personal Information
It is every person's responsibility to ensure that Personal Information is protected from loss or compromise. All persons who are granted access to Personal Information are responsible for protecting information from inappropriate disclosure, modification, misuse, or loss. On the departure date from GBLS, staff must return all files and records in any form containing Personal Information including all information stored on laptops, portable devices (such as thumb/USB/flash drives, CDs, DVDs, cell phones and PDA's), or any other type of media, or in files, records notes or papers.

Computer Systems Passwords
As a person authorized to use GBLS computer systems, including but not limited to PC's, laptops and network(s), you are assigned a unique user name (user ID) and password. You are personally ***accountable*** for all network and computer system access under that user ID. Sharing user credentials (username and password) with family, friends or colleagues is prohibited and subject to disciplinary action by GBLS subject to any applicable collective bargaining agreement.

To prevent unauthorized access to the GBLS computer systems or network, all persons are prompted by the system to change their passwords every 6 months. All passwords must meet industry standard complexity requirements:

- Be a minimum of 8 characters in length

- Not include your name
- Contain a combination of upper (A, B, C...) and lower case letters (a, b, c)
- Contain at least one (1) numeric (1,2,3) or special character (&, !, @)

Storing password information in an unencrypted electronic document which is saved to the GBLS network, any affiliate network accessed by GBLS computer systems, removable media, PDA's or local PC's is prohibited. Sending passwords via unencrypted email is prohibited. Notating and/or displaying user ids and passwords in an area where others can view, (e. g., sticky note on monitor, hanging on a wall, attached to keyboard) is prohibited. After 3 unsuccessful attempts to access your GBLS account, your ID and password is locked (inactivated) to prevent further attempts. In order to reactivate a locked account, contact the GBLS Help Desk.

Locking Screen Savers
Your PC is set with a password-protected, locking screen saver. This screen saver is set to lock the screen after 15 minutes of inactivity. Please contact the GBLS Help Desk if you have any questions.

E-Mail Security
- E-mail containing Personal Information sent to any e-mail addresses outside of GBLS must be encrypted. (Information on how to encrypt is available on the GBLS staff web-site or by emailing the GBLS Help Desk.)
- The use of Gmail, Hotmail, Yahoo or similar external/third-party email services (commonly known as "webmail") for GBLS business including Personal Information is prohibited.
- Forwarding or auto-forwarding email belonging to the Organization and containing personal information to external/third-party email services is prohibited unless the personal information is encrypted.
- E-mails or attached files should never be opened without ensuring that the content appears to be genuine. If you are not expecting to receive the message or are not absolutely certain about its source, do not open it.

Remote Access to the Organization's Resources
Remote access to the GBLS system may only be used to conduct legitimate business and not for personal use or by anyone not working for GBLS. You are responsible for protecting GBLS Personal Information while working remotely and bear responsibility for the consequences should this access be misused. It is the responsibility of every person with remote access privileges to ensure that their remote access connection remains as secure as his or her network access within their office.

Any remote computer used to connect to the Organization's network must have an up-to-date antivirus software installed and be protected by the latest operating system security patches available.

At no time while using a system that you do not control (e.g. a public computer) should you download or store Personal Information unless absolutely necessary for business purposes and only when the data downloaded has been encrypted using standard encryption methods approved and contained herein. Connections to the Organization's system shall not be left open and

unattended. If a remote pc is idle after four (4) hours, the account is automatically logged off and disconnected from the system.

Network Connections Wi-Fi
The data that is transmitting over a wireless network can easily be intercepted by unauthorized individuals who can create a serous security risk to Personal Information unless reasonable safeguards are taken. Home wireless networks which are setup by outside vendors such as cable companies are often configured with many vital security features disabled. Also, public "hotspots" are generally left unsecure to allow users easier access. For these reasons, persons are prohibited from obtaining access to Personal Information while using an unsecured wireless network connection except in emergencies when there is no reasonable alternative.

Laptop Security
Portable computers are especially vulnerable to physical damage or loss, and theft. The physical security of the laptop assigned to you by GBLS is your personal responsibility so please take all reasonable precautions. Laptops being used outside the usual work place should be locked away and out of sight when they are not being used. Do not leave your laptop visible in an unattended vehicle. If it is absolutely necessary to leave the laptop in an unattended vehicle, lock the laptop out of sight in the trunk or glove box but it is generally much safer to take it with you. GBLS laptops are installed with data encryption software, anti-virus and anti-malware software. Tampering, disabling or otherwise rendering this software's ability to encrypt the data update, scan or protect the data is prohibited.

Smartphone/ PDA Security
Because of their small size and use outside the office, handheld devices can be easier to misplace or be stolen than a laptop or notebook computer. If they do fall into the wrong hands, gaining access to the information they store can be relatively easy.

- Your smartphone or PDA must have a password.
- Storing unencrypted IDs or password on your PDA is prohibited
- Please do not save Personal Information to your handheld device (e.g. download GBLS email or files with Personal Information)

Storage
Electronic Personal Information stored on removable media or portable devices must be encrypted. This includes thumb drives, cd's, and laptops.

Paper records containing Personal Information shall be stored in a locked file cabinet or in a controlled area when unattended. Floors that are only accessible by pass code are considered controlled. Even in controlled areas, documents containing personal information should not left open in public areas such as student carrels, secretarial desks or library tables where they can be read by passersby.

Transmission
Personal Information transmitted outside the GBLS network, including but not limited to e-mail, uploading and downloading to internet sites and any other form of electronic transmission, must be encrypted in order to protect against unauthorized disclosure.

Transporting outside the Organization's premises
In the event it is necessary to transport Personal Information outside of GBLS's premises, special precautions must be taken prior to, during, and following transportation/travel. Only those physical documents/files which are necessary to accomplish legitimate business requirements shall be removed from GBLS's premises. Files and any other physical documents containing Personal Information removed from the office by students or interns must be recorded in a sign out log. Only removable media authorized by GBLS should be used to remove electronic Personal Information from the system. Authorized removable media are:

- Thumb/USB drives preconfigured with approved encryption.
- Full disk encrypted removal / portable hard drives.

Removable media may not be connected to or used in computers that are not owned or leased by GBLS without explicit permission from the PDIP Manager.

All authorized removable media used to store Personal Information must contain a serial number that is recorded by the PDIP Manager and signed out to the Covered Person so that it can be tracked and accounted for.

If any removable media which is known or suspected to contain Personal Information is lost or stolen it must be immediately reported to the PDIP Manager.

Disposal
It is the responsibility of every person to ensure that Personal Information they are responsible for is disposed on in a way that prevents the paper document from being read, reconstructed or used. Paper documents containing Personal Information must be redacted or shredded. CASLS and every floor at Friend Street has a shredder and a secure disposal bin. Electronic media including but not limited to computer hard drives, PDA's and removable media containing Personal Information shall be destroyed or erased so that Personal Information cannot practicably read, reconstructed or used.

IMPLEMENTATION POLICIES AND PROCEDURES:

The receipt and understanding of these policies shall be acknowledged by all GBLS computer users by signature below. GBLS reserves the right to make minor changes and issue implementation procedures to these policies with written notice to those to whom the measures apply but without the re-execution of this document.

Please sign and date and return this page to the Director of Human Resources, 5th floor

Read and acknowledged by:

Signature: _____

Print Name: _____

Date: _____