Gleaners Community Food Bank
Acceptable Use Policy

Overview:

Gleaners Community Food Bank's intention for publishing an Acceptable Use Policy is to support our mission of nourishing communities by feeding hungry people. Gleaners is committed to protecting our team, volunteers, consultants, donors, and partners, from illegal or damaging actions by individuals, either knowingly or unknowingly.

Gleaners provides team members with electronic devices, including but not limited to computers, USB drives, printers, telephones, cell phones, software, and network accounts for e-mail and other internet-based content and tools. These devices and systems are the property of Gleaners and are to be used for business purposes in serving the interests of the company, and of our partners and donors in the course of normal operations.

Effective security is a team effort involving the participation and support of every user who deals with information and or information systems. It is the responsibility of every user to know these guidelines and conduct their activities accordingly.

Purpose:

The purpose of this policy is to outline the acceptable use of computer and data equipment, applications, and services at Gleaners. These rules are in place to protect the employee and Gleaners. Inappropriate use exposes Gleaners to risks including virus attacks, compromise of network systems, and potential legal issues.

Scope:

This policy applies to anyone who is approved to use Gleaners equipment, including but not limited to: employees, contractors, consultants, volunteers, and temporary staff at Gleaners. It also applies to all equipment, software, and services that are owned or leased by Gleaners.

Policy:

General Use

While Gleaners desires to provide a reasonable level of privacy, users should be aware that data they create remains the property of Gleaners. Because of the need to protect Gleaners' network, management cannot guarantee the confidentiality of information stored on any network devices or internet resources belonging to or provided by Gleaners.

For security and network maintenance purposes, authorized individuals within Gleaners may monitor equipment, systems, and network traffic at any time.

Employees are responsible for exercising good judgment in the reasonableness of personal use for all devices and tools.

Security and Proprietary Information

Passwords

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

For more details, please find Gleaners' Password Policy located in *P:\Technology Information\Passwords*.

Wireless Access Points

Wireless network access points are password secured. This password should not be shared to the public unless authorized by the IT Department.

Email

Employees must use extreme caution when opening e-mail messages and attachments received from unknown senders as these may contain viruses, e-mail bombs, or other malware. This includes accessing personal e-mail accounts with Gleaners' equipment. When using e-mail, all company related business must be conducted on the Gleaners provided e-mail account.

Data File Storage

Gleaners' related data must be stored on a network server for security and retrieval purposes. See the Network Drives document located in *P:\Technology Information\Network Drives* for network drive descriptions and protocol.

Electronic Equipment

Reasonable care should be taken to keep Gleaners' electronic equipment in a safe, temperature controlled environment. Read the Equipment Storage and Maintenance document located in *P:\Technology Information\Care of Electronic Equipment* for guidelines on the proper storage and maintenance of electronic equipment.

Staff is welcome to borrow company issued equipment like laptops and audio and visual (AV) equipment for special events. Please submit your equipment request to the IT Department via the ticketing system.

Remote Access

Remote access to Gleaners network resources is available. Instructions for logging onto the terminal server (TS) to access the network are located in *P:\Technology Information\TS*. Instructions for logging onto Webmail to check your email, contacts, and calendar appointments are located in *P:\Technology Information\Webmail*. To access the network file shares and all of your Gleaners' applications on your work computer please see the Dell SonicWALL NetExtender document located in *P:\Technology Information\Dell SonicWALL NetExtender*.

Security Risks

The IT Department tracks and documents incidents related to security risk. If you see something that concerns you, even if you aren't sure that it is a problem, please report it to the IT department through the ticketing system. To file a more formal report about a specific incident, you can find the IT Security Risk Form located in *P:\Technology Information\Forms*.

Volunteers

Volunteers utilizing the Gleaners network are required to have a background check prior to accessing the network.

Unacceptable Use

Under no circumstances is an employee of Gleaners authorized to engage in any activity that is illegal under local, state, federal or international law while using Gleaners-owned resources.

Violations of the rights of any person or company protected by copyright, trade secrets, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Gleaners.

Personal Computer Files and Software

Gleaners prohibits the installation and use of personal computer software "brought from home" on company-owned computers unless authorized by the IT Department.

Without the explicit approval of management, the transfer of files and/or data in-between personal and work computers is prohibited.

The sole storage of work-related files on personal electronic devices which include computers, tablets, and smart phones is prohibited as it puts Gleaners data at risk of loss.

Software Assurance

Software licensed by Gleaners may be used on a home computer only when specifically authorized by the IT Department.

Copyright Materials

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Gleaners or the end user does not have an active license is strictly prohibited.

Viruses, Worms, Trojans, etc.

Intentional introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.)

Passwords

Do not reveal your account password to others or allow others to use your account. Please review the Password Policy document located in *P:\Technology Information\Passwords* for a summary on individual network logins.

Inappropriate Images

Using a Gleaners device to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws. Please review the Inappropriate Images document located in *P:\Technology Information\Inappropriate Images* for a summary of Inappropriate Images on Computer Screens.

Fraudulent Offers

Making fraudulent offers of products, items, or services originating from any Gleaners account.

Streaming Audio/Video

Streaming of business-related video and audio is acceptable. However, if the bandwidth at any site becomes overused due streaming activities, then the IT Department has the authority to block the streaming activity.

Security Breaches

Effecting security breaches or disruption of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not authorized to access. Please refer to the Network Drives document located in *P:\Technology Information\Network Drives* for instructions and protocols regarding creating and using public files for limited and network wide access.

Circumventing user authentication or security of any host, network, or account.

Interfering with or denying service to any other user.

Providing unauthorized or confidential information about, or lists of donors, agencies, volunteers, team members to parties outside of Gleaners.

The extraction and storage of business-related data solely on personal electronic equipment is prohibited.

Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of message.

Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type.

VPN Access - Vendors and others

All vendors and specialized volunteers needing access to the network are required to utilize an IT authorized VPN connection. Please request this access with the IT Department through the ticketing system.

Blogging & Social Networking

Limited use of Gleaners’ systems to engage in blogging and social networking is acceptable, only as part of a normal work activity, and only if done in a professional and responsible manner, it does not violate Gleaners policy, and is not detrimental to Gleaners’ best interests. Activities performed on Gleaners’ systems are subject to monitoring.

Gleaners’ confidential information policy also applies to blogging and social networking. As such, employees are prohibited from revealing unauthorized information about donors, agencies, volunteers, and team members.

Employees shall not engage in any blogging and social networking that may harm or tarnish the image, reputation and or goodwill of Gleaners and/or any of its employees. Employees are also prohibited from making discriminatory, disparaging, or defamatory comments when blogging and social networking or otherwise engaging in any conduct prohibited by Gleaners' Non-Discrimination and Anti-Harassment policy.

Opinions expressed must be designated as personal opinions that do not represent the views of Gleaners in any manner.

Internet Usage

Misuse of the internet can occur in many ways, such as:

The wasting of work time by performing unauthorized research or accessing non-business related information and people. *[Reasonable non-commercial personal use of the internet may be allowed provided it does not interfere with work or violate the computer use policy. Employees are encouraged to limit their personal use of the internet to breaks and lunch hours.]*

Downloading files or applications from the internet without prior IT authorization.

Creating or implementing public access databases without prior IT authorization.

Use of the internet for partisan political purposes.

Use of aliases or transmission of anonymous messages; additionally, Internet users must not misrepresent their job titles, job descriptions, or positions.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.