

Acceptable Use Policy (AUP)



Version number	10.4
Last Approved	Mar 28, 2024
Classification	PUBLIC

Learning Technologies Group plc – Proprietary and Confidential – This document contains confidential information, which is the property of Learning Technologies Group plc, and may not be distributed externally without explicit written permission.

Overview

The Acceptable Use Policy (AUP) stipulates constraints and practices that Company Personnel must abide by while accessing and using The Company's resources and data, or client data. This policy covers areas which include but are not limited to: hardware, software, email and messaging, data storage, PII, internet, wireless networking, blogging, social media, and third party services.

Applicability

The applicability of this statement falls under purview of the [Security Documentation Overview](#).

Purpose

This Acceptable Use Policy provides guidelines for the use of computing resources and considerations on appropriate use of Company and customer data to ensure compliance with applicable laws and regulations.

Scope

This policy applies to all Personnel working with the Company's data or data provided by the customer for use in providing services.

In the event of conflicting obligations between Company policy and contractual requirements, the more stringent shall be applicable in the handling of customer data.

Acceptable Use Policy

Personnel must use IT Resources in an approved, ethical, and lawful manner in compliance with this AUP and other Company policies and procedures, to avoid damage to The Company and its customers. Personnel must contact a member of the Security Team or Management to report suspected violations of this AUP.

The Company provides access to IT Resources (e.g., desktop computers, laptop computers, servers, smart-phones, networking equipment, etc.) to facilitate the completion of Company business. Care must be taken to ensure the safety and security of these resources. Personnel who have been issued IT Resources are responsible for the physical security of those resources, regardless of where they are used (e.g.,

Company offices, residences, hotels, conference rooms, cars, airports, etc.). Personnel should adhere to a “clear desk/clear screen” protocol.

IT Resources and Company data stored are Company owned assets. Any damage or theft to Company assets found to be caused by gross negligence of the person to whom the asset was assigned will be recovered by The Company from the Personnel responsible.

Prohibitions

Generally prohibited activities when using IT Resources include, but are not limited to:

- Stealing or copying electronic files without permission.
- Establishing personal shares on (or otherwise sharing access to) local computing systems. Personnel with a business need to share access to data should contact Corporate IT Operations to determine an appropriate location.
- Stealing Company-owned property. All Company property assigned to Personnel must be returned promptly upon termination or upon The Company's request.
- Violating the rights of any person or company protected by copyright, trade secret, patent, intellectual property laws, or similar laws or regulations; including, but not limited to installing or distributing “pirated” software or other software products that are not appropriately licensed for use by The Company.
- Unauthorized copying of copyrighted material, including but not limited to: digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or movies; or the installation of any copyrighted software for which The Company does not have an active license.
- Exporting software, technical information, or encryption software or technology in violation of international or regional export control laws. The appropriate management should be consulted prior to exporting any material that is in question.
- Revealing account passwords to others or allowing the use of an account by anyone other than the individual to whom it is assigned. (This includes family and other household members when work is being done at home.)
- Using someone else's account and password. The use of “shared” or “group” Accounts to access Company or client assets is prohibited unless the VP Information Security grants an explicit written exception.
- Making statements about warranties (expressed or implied) unless it is a part of normal duties.
- Browsing the private files or accounts of others, except as approved by the VP Information Security or the LTG Sr. IT Manager.
- Performing unofficial activities that may degrade the performance of networks and systems (e.g., playing electronic games, excessive use of internet based audio and video streaming programs, etc.) except where required for completion of duties, organizational communication functions, or training purposes.
- Performing activities intended to circumvent security or the access controls of any organization, including the possession or use of hardware or software tools intended to defeat software copy protection, discover passwords, identify security vulnerabilities, decrypt files, or compromise information security by any other means.
- Breaching security or “disrupting” network communications. (For purposes of this section, “disrupting” includes, but is not limited to: network sniffing, ping floods, packet spoofing, denial of service, and forging routing information for malicious purposes.) Security breaches include, but are not limited to: intentionally accessing data or logging into a server or account to which Personnel are not expressly authorized (unless these actions are within the scope of regular duties); writing, copying, executing, or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of (or access to) any Company computer, network, or information.
- Accessing the Company network remotely via access methods not approved by the Company.
- Executing any form of network monitoring which intercepts data not intended for the Personnel's host (unless this activity is a part of the Personnel's normal duties).
- Discrediting or harming the reputation of The Company, its Personnel, or its business partners. This includes, but is not limited to making defamatory statements about The Company or its employees on Internet message groups.
- Using Company IT Resources to promote or maintain a personal or private business, or for personal gain.
- Conducting fraudulent or illegal activities, including but not limited to: gambling, trafficking in drugs or weapons, participating in terrorist acts, or attempting unauthorized entry to any Company or non-Company computer.

- Conducting fundraising, endorsing any product or service, lobbying, or participating in any partisan political activity using Company IT Resources.
- Disclosing any Company information that is not otherwise public.
- Performing any act that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in a false light, The Company or any person.
- Using Company IT Resources to perform any other activities that are in violation of Company policies.

Passwords

Administration

- Administrative passwords for Company computing systems (e.g., workstations, email servers, etc.) or other resources designated by the LTG Sr. IT manager, are managed by Director of IT.
- Administrative passwords for production and pre-production development and testing computers and networking systems, or other resources designated by the VP Information Security, are managed by Global Technology Operations (“GTO”).
- Administrative passwords for all Company security systems (firewalls, ACS, etc.) are managed by the Security Team.
- Passwords must be changed immediately when an account is believed to be compromised.

Complexity

All passwords utilized to authenticate access to Company computers and networking systems or to secure data files or data storage devices will conform to the following requirements:

- Passwords must be non-trivial and comply with “strong password” criteria:
 - May not be reused for 24 iterations
 - Be at minimum 8 characters
 - Contain characters from at least three of the following categories:
 - Uppercase English alphabet (A through Z)
 - Lowercase English alphabet (a through z)
 - Arabic numerals (0 through 9)
 - Non-alphanumeric characters: ~!@#%&*+`=^| \ () { } [] ; : " ' < > , . ? /

 Password requirements are enforced by Active Directory and LDAP security policy settings where applicable.

- All system level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on a regularly scheduled basis, not to exceed annually.
- All Production and Pre-Production system level passwords must be stored in the Global Technology Operations secure password management database.
- All user level passwords (e.g., email, web, desktop computer, etc.) must be changed on regularly scheduled basis, not to exceed 90 days.
- All Company system level passwords must be stored in the Corporate IT Operations secure password management database.
- User accounts that have system level privileges granted through group memberships (e.g., programs such as "sudo") must have a password unique from all other accounts held by that user.
- Where SNMP is used, community strings must be defined as something other than the defaults ["public", "private", and "system"] and must be different from any passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops, and workstations must be secured with a password-protected screensaver with an automatic idle-timeout feature set to 15 minutes or less, or by logging-off.



Account management policies and configuration on Company computers and networking systems will enforce an automatic account lockout for a period of 30 minutes after 10 failed login attempts, within a period of 30 minutes from the first attempt.

Hardware

Use of Personally-Owned Hardware

To protect IT Resource integrity, Personnel must NOT connect personally owned hardware to IT Resources. This includes peripheral devices such as PDAs, GPS systems, wireless networking devices, scanners, etc. If business needs dictate the necessity of such a device, Personnel must acquire the approval of Corporate IT Operations prior to the connection and use of the device.

Additionally, Personnel must NOT connect non-Company-owned computers or computing devices to any Company networks (except to designated "Guest Networks"). This includes computers owned by an individual or another corporation; networking hardware such as routers, hubs, switches, wireless access points, etc.; or any other computing device. This restriction applies to computers physically connected to a Company network (in a Company office) as well as those connected remotely (VPN). All exceptions must be approved by the VP Information Security.

Personnel may use personally-owned computers to connect to Company webmail including Smartphones via ActiveSync. However, Personnel should not connect to webmail from computers that they do not control (e.g., public terminals, kiosks, etc.) except in emergency situations where no other method of communication is possible. Personnel may not use personally-owned external storage devices to capture, transport, or store data of any kind from Company-owned computer systems.

Software

To prevent the introduction of malicious code and to protect IT Resource integrity, all hardware and software must be obtained from official Company sources, per the applicable purchasing policy. Introduction of any hardware or software into The Company's computing environments must be approved by Corporate IT Operations.

All software that runs on a Company-owned computing device must be approved and installed by Corporate IT Operations. Personnel must not install any software on computing devices without approval from Corporate IT Operations. Any non-approved software found running on a Company-owned computing device will be removed at the time of discovery.

Copyright and Licensing Compliance

Background

The Company purchases, licenses, and tracks software from a variety of sources that are previously vetted and then considered authorized providers. Any duplication or alteration of software, except as permitted by related license agreements, is a violation of federal law and is therefore prohibited. (Unauthorized installations also place The Company and its Personnel at risk for civil action, which can result in punitive measures imposed on all involved parties.)

Licensing and Installing Software

Company Personnel purchasing or using computer systems for work-related purposes must adhere to the following conditions:

- Purchase, install, and use only software that has been authorized for use on Company computers by CITO.
- Procure all software to be used on IT Resources in accordance with official Company policies and procedures.
- License and register all software in The Company's name.
- Obtain proper invoicing or payment receipts (and licensing documentation) for all work-related software purchases, as defined in the company's Expense Reimbursement and Travel Policy.
- Provide Corporate IT Operations a copy of all software licenses for asset registration and inventory management.
- Abide by software copyright laws and the terms of all license agreements as they pertain to the use of software on Company-issued computers.


- Do not duplicate, reproduce, or install software on more than one machine without prior written authorization from Corporate IT Operations.
- If a software license states it is eligible and approved for home use, the user must adhere to the following conditions:
 - Use of the software is limited to Company Personnel.
 - Software must be removed upon separation from The Company.

Use of Personally-Owned Software

To protect IT Resource integrity, Personnel must not use personally owned software on IT Resources without the approval of Corporate IT Operations. This includes purchased applications; shareware; freeware; downloads from bulletin boards, the Internet, Company Intranet, FTP sites, local area networks (LANs) or wide area networks (WANs); and other personally owned or controlled software.

Monitoring

To ensure adherence to software usage policies and related federal laws and statutes, The Company reserves the right to monitor software installation and usage on all Company IT Resources, as well as any privately owned computers when used to conduct Company business.

 Corporate IT Operations conducts ongoing scans of all IT Resources for installed software and licensing information. Any unlicensed or unauthorized software is removed (or licensed appropriately).

Protection of Intellectual Property

To ensure the integrity of Company developed software, all personnel must abide by the requirements for protecting (and the proper usage and disclosure of) proprietary Company data, as stated in The Company's [Data Classification Policy](#).

Electronic Mail and Messaging


Company Property


As a productivity enhancement tool, The Company encourages electronic communications. (e.g., the Internet, voicemail, electronic mail, fax, etc.) Company electronic communication systems and all messages generated on them or handled by them (including back-up copies) are considered the property of The Company.

Authorized Usage

Company electronic communication systems should generally be used only for business activities. Incidental personal use is permissible as long as it:

- Does not consume more than a small amount of resources,
- Does not interfere with Personnel productivity, and
- Does not preempt any business activity.

 Personnel are forbidden from using The Company electronic communication systems for charitable endeavors, private business activities, or other activities for personal gain.

 The use of Company resources, including electronic communications, must never be inappropriate (or create the appearance of impropriety).

Default Privileges

Privileges on electronic communication systems must be assigned such that only those capabilities necessary to perform a job are granted. (e.g., End-users should not be authorized to reconfigure electronic mail system software.)

User Accountability

Regardless of the circumstances, individual passwords must never be revealed to anyone besides the authorized user. (Doing so exposes the authorized user to the responsibility for any actions the other party takes with that password.)


If Personnel need to share data, they must utilize message forwarding facilities, public directories located on network servers, or other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, Personnel must choose nontrivial passwords which comply with the *Password Complexity* section of this document.

User Identity

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communication system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator.

No Default Protection

Company electronic communication systems are not encrypted by default; and sensitive information should not be communicated unencrypted.

 If sensitive information must be sent via electronic communication, Personnel should contact the [Security Team](#) to determine an appropriate encryption method (or similar technology) to protect the data being sent.

Respecting Privacy Rights

Personnel may not intercept, disclose, or assist in intercepting or disclosing electronic communications (unless this activity is a part of the Personnel's normal duties).

The Company is responsible for servicing and protecting its electronic communication networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications. Therefore, Company Personnel should have no expectation of privacy while using electronic communication equipment furnished by The Company.

No Guaranteed Message Privacy

The Company also cannot guarantee that electronic communications will be private. Depending on the technology, electronic communications can be forwarded, intercepted, printed, and stored by others. Furthermore, (at times) other Personnel can access electronic communications in accordance with this policy.

Regular Message Monitoring and Copies

It is not the policy of The Company to regularly monitor electronic communications. However, the content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Personnel should structure their electronic communications in recognition of the fact that Company system administrators will from time to time examine the contents of electronic communications (as directed by Security, Human Resources, or IT management).

The Company also reserves the right to make copies of all incoming and outgoing electronic mail messages.

Statistical Data


Consistent with generally accepted business practices, The Company collects statistical data about electronic communications (e.g., call information collected by telephone switches indicates the numbers called, call duration, time of day, etc.). Technical support Personnel use this information to ensure the ongoing availability and reliability of IT Resources.

Incidental Disclosure

During the course of problem determination, it may be necessary for technical support Personnel to review the contents of individual Personnel's communications. Technical support Personnel may not review the content of any communications out of personal curiosity or at the behest of individuals without the authority to request such activity.


Message Contents

Personnel must not use profanity, obscenities, or derogatory remarks in electronic mail discussing Personnel, customers, competitors, or others. Such remarks, even when made in jest, may create legal problems such as trade libel or defamation of character.

 Extra caution is warranted because backups and archived copies may actually make emails more permanent and more readily accessible than traditional paper communications.

Message Forwarding

Some information is intended for specific individuals and may not be appropriate for general distribution. Therefore, Personnel should exercise caution when forwarding messages. Company sensitive information must not be forwarded to any party outside The Company without the prior approval of a local department manager.

 Mass forwarding of messages to parties outside The Company is prohibited unless approved by Corporate IT Operations management.

Security Incident Reporting

Personnel must promptly report all alarms, information security alerts, warnings, suspected vulnerabilities, and the like to the IT Help Desk or the Security Team. All Personnel are responsible for being aware of (and following) The Company's [Security Event/Incident Response Plan](#) in order to help ensure proper actions are taken to maintain data integrity, accountability, and employee safety.

Public Representations

No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message, or any other public representation about The Company may be issued unless it has first been approved by the Marketing Department.

User Back-Up

If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of a Company management decision, it must be retained for future reference. Most electronic mail messages will not fall into these categories and accordingly can be erased after receipt. Users must regularly move important information from electronic mail message files to Word processing documents, databases, or other files. Electronic mail systems are not intended for the archival of important information. (Important stored electronic mail messages can be periodically purged by systems administrators or mistakenly erased by users.)

Purging Electronic Messages

Except those messages maintained in accordance with The Company's then-current back up policies and procedures, messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period (generally six months) electronic messages stored on multi-user systems will be automatically deleted by systems administration staff. Not only will this increase scarce storage space, it will also simplify records management and related activities.

Harassing or Offensive Materials

The Company's computers and communications systems are not intended to be used for, and must not be used for the exercise of Personnel's right to free speech. Any form of harassment including unwanted telephone calls, electronic mail, and internal mail is strictly prohibited and may be cause for disciplinary action up to and including termination. Personnel are encouraged to respond directly to originators of offensive electronic mail messages, telephone calls, or other communications. If the originator does not promptly stop sending offensive messages, Personnel must report the communications to their manager and to Human Resources. The Company retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Proper Data Storage


Clients and partners entrust The Company with sensitive information related to their businesses. The nature of this custodianship requires strict confidentiality; any disclosure of sensitive information could adversely affect The Company's business relationships, position in the technology community, and competitive advantage.

Personnel are required to protect Confidential Information with good judgement and the highest ethical standards as well as guard against its inadvertent disclosure. More specifically, Personnel are required to store Confidential Information only in secured locations (on secured servers) and not on portable devices.

Portable Media

To ensure that Confidential Information is not placed at unnecessary risk, The Company restricts the use of portable storage devices (i.e., flash drives, external USB drives, DVD burners, etc.) Personnel are prevented from writing to portable media on Company owned devices.

 Reading from portable media is allowed.

 Personnel whose job role requires writing data to portable media are exempt. Any other personnel wishing to write to portable media must have approval from two lines of management and the Chief Information Security Officer. (Contact [Security](#) for instructions on acquiring an exception.)

Whenever writing data to portable media, full-disk encryption (via BitLocker) is required.

Cloud Storage

The Company embraces using cloud solutions, including cloud storage. However, not all cloud storage solutions are equal. They vary widely both in security features and their providers' underlying security practices.

To protect clients' privacy as well as to reduce the risk of any data "leakage", The Company requires the use of **Company-administered cloud solutions** (only) when writing data to the cloud.

Internet

Access to the Internet is available to Personnel whose duties require it for the conduct of Company business. Since Internet activities may be monitored, all Personnel accessing the Internet should have no expectation of privacy.

The Company provides Internet access to facilitate the conduct of Company business. Occasional and incidental personal Internet use is permitted if it does not interfere with the work of Personnel, the Company's ability to perform its mission, and the conditions outlined in this policy.

Prohibited activities while using the Internet include, but are not limited to:

- Browsing pornographic or hate-based web sites; posting, sending, or acquiring sexually explicit or sexually oriented material, hate-based material, or other material determined to be prohibited (except where required by duties for monitoring or policy enforcement, for which management approval is required)


- Browsing hacker or cracker websites; posting, sending, or acquiring hacker or cracker-related material, or other material that The Company has determined to be prohibited (except where required by duties for monitoring or policy enforcement, for which management approval is required)
- Participating in newsgroups or discussion websites using a Company email address (even for work-related discussions)
- Posting or sending sensitive information outside the corporation without management authorization
- Using Instant Messaging applications or protocols other than those managed by Corporate IT Operations. (The use of AOL Instant Messenger, Yahoo Messenger, MSN Messenger, Jabber, IRC, ICQ, or other Instant Messaging clients or services is strictly prohibited.)
- Installing or using any 'peer-to-peer' file sharing software (e.g., Kazaa, Morpheus, Limewire, Gnutella, Bittorrent, etc.)
- Installing or using any 'distributed computing' software (SETI@home, distributed.net, Lifemapper, etc.)
- Engaging in excessive use of internet-based streaming audio or video programs (except where required for completion of duties, organizational communication functions, or training purposes)
- Initiating data transfer (e.g., FTP, SCP, Telnet, SSH, VPN, etc.) with foreign systems or networks unless required to perform Company sanctioned functions (e.g., receiving patch updates, uploading debug files, etc.). Inbound VPN and SSH connections initiated from foreign networks must be approved by Security prior to attempting connection.
- Posting or hosting non-Company related commercial announcements or advertising material on Company computer information systems or networks
- Using Company resources to maintain a personal or private business
- Receiving news feeds or pushing data updates on subjects that are not related to The Company, your job, or career enhancement
- Using the Internet to perform any other activities which are in violation of Human Resources policies

Wireless Networking

Acceptable Wireless Use

The use of wireless networking is acceptable for conducting Company business in the following situations:

- Connecting to Company networks while attending Company functions outside normally assigned work areas (e.g., meetings and interviews).
- Connecting to Company networks while at other venues (e.g., hotels, external meetings, etc.) where no other means of network access is available.
- Connecting at home, where security measures have been implemented to secure and limit access to the wireless network (WPA or WPA2 wireless encryption)

 Wireless networking must not be used to access production networks.

All connections to Company computing resources (other than Webmail) made from home or other non-Company locations (where The Company's wired or wireless network is not available) must be made via VPN.

 In the absence of a VPN connection, the transmission of Company data over unsecured Wi-Fi is prohibited.

Prohibited Wireless Use

Prohibited activities when using Wireless networking include, but are not limited to:

- Connecting wireless access points to Company-owned networks. (Wireless access points may only be connected to Company-owned networks by Corporate IT Operations.)
- Using PC-to-PC wireless connections

 Connecting Company-owned devices to a wireless network for non-business use is strictly prohibited.


 All exceptions to the Wireless Networking provisions of this policy must be approved by Corporate IT Operations management.

Mobile Devices

Mobile devices are highly attractive targets for theft and attempted compromise. Care must be taken to secure mobile devices not only because of their monetary value, but also because of the sensitive data stored therein.

Physical Security

Specific actions must be taken by all Personnel who have a Company-issued mobile computing device (e.g., desktop, laptop, tablet, smartphone, etc.) or who are temporarily using a “shared” Company mobile device.

 Personnel must secure all mobile devices when they are not being used.

- All mobile devices acquired for (or on behalf of) The Company are deemed Company property.
- All Personnel issued a mobile device are responsible for the security of their mobile device, regardless of if it is used in the office, at a place of residence, or in any other location (e.g., hotel, conference room, car, or airport).
- Mobile devices (excluding desktops) that are not taken home after working hours must be secured in a locked cabinet, drawer, or secure office. Leaving a mobile device in a docking station or on a desk is **NOT** acceptable.
- While traveling, mobile devices must not be left unattended at any time while powered on. If left in a hotel room, they must be powered off and not left in plain sight, but placed in a concealed location (e.g., drawer, closet, under the bed, etc.). If provided, hotel room safes or secure cabinets must be used to store mobile devices or mobile device hard drives.
- When traveling, mobile devices must not be checked in with luggage. Keep mobile devices with you at all times.
- If a mobile device must be left in a vehicle it must be secured in a trunk (in the case of cars) or behind the seat with locked doors (in the case of trucks).
- Mobile devices (excluding desktops²) that will not be used for several days must be locked out of sight in a secure cabinet or safe.

Security Controls

Subverting installed security software or security settings on any Company device is strictly prohibited (except where required by Personnel's normal duties, for which Corporate IT Operations Team or Security Team approval is required).

Sensitive Data on Mobile Devices

Personally Identifiable Information (“PII”: e.g., Social Security Numbers, credit card numbers, driver's license numbers, etc.) must never be stored on mobile devices that do not have company sanctioned full disk encryption software installed. (This includes USB drives.)

Responsibility


Mobile devices are company owned assets; therefore, any damage or theft found to be caused by reasons other than normal “wear and tear” (e.g., misuse or neglect in taking proper security precautions) will be recovered by The Company from the Personnel to whom the device was issued.

Access

General

- Personnel must never leave mobile devices unlocked. Screen-locking mechanisms must be engaged on unattended devices. (Disconnecting from any active VPNs is also recommended.)
- Mobile devices that connect to company email systems must have an idle “time-out” lock, with:
 - A maximum 15 minute idle time-out

- A minimum 4-digit PIN authentication

 Finger swipe PIN systems are not an acceptable means of authentication.

Home Access

- Mobile devices that are taken home must not be left connected to the Internet when not in use.
- Mobile devices that are taken home must not be utilized for anything other than company business. (They must not be left unattended where family members or visitors have access to them.)

Mobile Phone Numbers

Personnel may be issued a telephone number (or be allowed to provide their own telephone number) for use on their Company-issued Smartphone. Upon assignment, these phone numbers become the property of The Company; Personnel rescind any and all rights to ownership of these numbers.

Provisions Applicable to PII

Personnel who receive, store, process, or otherwise has access to personal information at any time while performing their Company duties must comply with the provisions of this section.

“Personal Information” means an individual's first and last name or first initial and last name in combination with any one or more of the following:

- social security number
- driver's license number or state-issued identification card number
- financial account number
- credit or debit card number

Records containing Personal Information must be kept in the strictest confidence and all mobile devices (including flash drives, cell phones, external hard drives, and USB data drives) that contain Personal Information must employ full disk encryption technology. Personnel that receive, store, maintain, process or otherwise have access to Personal Information must confirm with the Information Security Manager no less than once annually that the appropriate encryption technology is present on their mobile device(s). Personnel must never receive, store, maintain, process or otherwise access Personal Information if they are unsure whether or not encryption technology is present on their mobile device(s). Personnel may contact IT Support for verification of encryption status of their laptops, as only Company-licensed encryption software solutions are deemed acceptable solutions for this requirement.

Accessing, transmitting or transporting Personal Information is only allowable if:

- duly authorized for a lawful purpose
- strictly necessary in the performance of Personnel duties
- in accordance with applicable law

If Personal Information is no longer necessary for performing Personnel duties, it must be promptly and permanently deleted from all Personnel computing devices.

The Company will regularly offer training courses related to compliance with the provisions in this section. Personnel that receive, store, maintain, transmit, process or otherwise have access to Personal Information must participate in relevant training courses (that are made available by The Company, at Company's cost) when requested.

All Personnel must promptly report any breach or suspected breach of security, or violation of the provisions contained in this section to the VP Information Security. All email communications referencing Personal Information control violations must carbon copy The Company's General Counsel.

Failure to adhere to the requirements of this policy or failure to take adequate data privacy precautions could result in negative consequences for all parties involved. This includes the individual and the client organization whose data has been mishandled, The

Company, and the Personnel who may have been at fault.

Possible consequences can include the following:

- identity theft suffered by users of Company services and Company employees
- financial and credit loss, psychological damage as result of identity loss
- public embarrassment and damage to The Company's reputation
- loss of business productivity due to interruptive investigations and remediation efforts
- possible regulatory and civil fines levied against The Company
- possible criminal prosecution brought against The Company and individually against negligent Personnel

Access Termination

Physical and logical access must be removed immediately upon notification (from Human Resources or management) of employment termination or changes in: job role, authorization for access to PII, Company office spaces, or data center access requirements.

Blogging and Social Media

General Provisions

The Company takes no position on Personnel's decision to start or maintain a blog. However, it is the right and duty of The Company to protect itself from unauthorized disclosures of information. The Company blogging policy includes rules and guidelines for Company-authorized blogging and personal blogging and applies to executive officers, board members, management, and non-management Personnel.

Unless specifically authorized by The Company to do so (as part of an employee's duties) Personnel must not blog or use other forms of social media or technology on the Internet during working hours or at any time on Company IT Resources. Blogging or other forms of social media or technology include, but are not limited to: video or wiki postings, social networks, virtual worlds, chat rooms, personal blogs or other similar forms of online journals, diaries, or personal newsletters not affiliated with The Company.

Unless specifically instructed, Personnel are not authorized to (and are therefore restricted from) speaking on behalf of The Company. Personnel may not publicly discuss clients, products, Personnel, or any work-related matters, whether confidential or not, outside Company-authorized communications. Personnel are expected to protect the privacy of The Company and its Personnel and clients and are prohibited from disclosing personal employee or non-employee information or any other proprietary or non-public information to which Personnel have access. Such information includes, but is not limited to: customer information, trade secrets, financial information, and strategic business plans.

Employer Monitoring

Personnel should have no expectation of privacy while using the Internet. Postings can be reviewed by anyone, including The Company.

The Company reserves the right to monitor comments or discussions about itself, its Personnel, its clients, and the industry (including products and competitors), posted by anyone (including Personnel) on the Internet. The Company may use blog-search tools to monitor forums such as blogs, social and virtual worlds, personal journals, diaries, and personal and business discussion forums.

Personnel should have no expectation of privacy while using IT Resources for any purpose, including authorized blogging. The Company reserves the right to use content management tools to monitor, review, or block content on Company blogs that violate Company blogging rules or guidelines.

Reporting Violations

The Company strongly urges Personnel to report any violations or possible violations of this policy to managers, Security, or Human Resources. Violations include discussions of The Company or its Personnel or clients, discussions of proprietary information, and any unlawful activity related to blogging.

Discipline for Violations of social media guidelines

The Company investigates and responds to all reports of violations of the social media provisions of this policy and other related policies.

Violations of Company social media policy will result in disciplinary action up to and including termination. Discipline or termination will be determined based on the nature and circumstances of social media posts. The Company reserves the right to take legal action where necessary against Personnel who engage in prohibited or unlawful conduct.

Authorized Blogging

The goal of authorized blogging is to become a part of the industry conversation and promote the web-based sharing of ideas and exchange of information. Authorized blogging is used to:

- convey information about Company products and services
- promote and raise awareness of The Company brand
- search for potential new markets
- brainstorm with Personnel and customers
- issue or respond to breaking news or negative publicity
- discuss Company, business-unit, or departmental activities and events

When blogging or using other forms of web-based forums (whether used inside or outside the workplace) The Company must ensure that these communications maintain its brand identity, integrity, and reputation, while minimizing actual or potential legal risks.

Rules and Guidelines for “Authorized Blogging”

The following rules and guidelines apply to blogging when authorized by the employer and done on Company time. These rules and guidelines apply to all employer-related social networking sites, including employer subsidiaries or affiliates.

Only authorized Personnel may prepare and modify content for Company social networking sites. Content must be relevant, add value, and meet at least one of the specified goals or purposes listed in “Authorized Blogging.” If Personnel are uncertain about specific information, material, or conversations, they should discuss the content with their manager, Corporate IT Operations, or Human Resources.

All Personnel must identify themselves as employees of The Company when posting comments or responses on The Company’s social networking sites. No copyrighted information may be posted on The Company’s social networking sites without written reprint preapproval. Authorized Personnel may remove any content that does not meet the provisions of the social networking policy or that may be illegal or offensive. Removal of such information will be done without the blogger’s permission or advance warning.

The Company expects all guest bloggers to abide by all rules and guidelines of this policy as well as other applicable Company policies. The Company reserves the right to remove (without advance notice or permission) all guest bloggers’ content considered to be inaccurate or offensive. The Company also reserves the right to take legal action against guests who engage in prohibited or unlawful conduct.

Personal Blogs

The Company respects the right of Personnel to use blogs and does not want to discourage Personnel from self-publishing and self-expression. Personnel are expected to follow the guidelines and policies set forth to provide a clear line between Personnel as an individual and Personnel as the employee, contractor, subcontractor, etc. (as applicable). The Company does not discriminate against Personnel who use these mediums for personal interests and affiliations or for other lawful purposes.

Bloggers are personally responsible for their commentary. Bloggers can be held personally liable for commentary that is considered defamatory, obscene, proprietary, or libelous by any offended party, not just The Company.

Personnel must not use Company-owned equipment, including computers, Company-licensed software, or other electronic equipment (nor may they use Company facilities or Company time) to conduct personal blogging. Personnel may not use social media to harass, threaten, discriminate, or disparage Personnel or anyone associated with or doing business with The Company.

If bloggers chooses to identify themselves as Company Personnel, some readers may view the blogger as a Company spokesperson. Therefore, The Company requires that bloggers state that their views are the blogger’s own (and not those of The Company or of any

person or organization affiliated or doing business with The Company).

Personnel may not post on personal blogs the name, trademarks, or logos of The Company or any business with a connection to The Company. Personnel must not post Company-privileged information, including copyrighted information and Company-issued documents.

i Personnel are reminded of the applicable confidentiality obligations between Personnel and The Company.

- Personnel must not post on personal blogs:
 - photographs of other Personnel, clients, vendors, or suppliers
 - photographs of persons engaged in Company business or at Company events
 - photographs of Company products
- advertisements of Company products
- Personnel must not sell Company products and services on personal blogs.
- Personnel must not link from a personal blog to The Company internal or external websites.
- If contacted by the media or press about personal blog posts related to The Company, Personnel must contact The Company's Public Relations Manager before responding.

Ensuring Compliance

The Company owns all IT Resources, and these resources remain the property of The Company while assigned to Personnel for their use in conducting Company business. Use of Company IT Resources constitutes the Personnel's consent for The Company to monitor, inspect, audit, collect, or remove any information without permission or further notice. Personnel will be informed as to what use is acceptable and what is prohibited. Any infraction of Company acceptable use policies constitutes a policy violation, for which Personnel will be held personally accountable.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the [Security Documentation Overview](#).

Document control

i This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @Sarah Zwicker (Unlicensed) @John Cole	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Mar 28, 2024
Review cycle	ANNUAL	
Next review date	Mar 28, 2025	

Version History

Date	Author(s)	Version	Changes
Nov 01, 2024	@angelina.kilmer	10.4	Updated Policy classification from Confidential to Public
Mar 28, 2024	@Art Machado @Sarah Zwicker (Unlicensed) @Paul Gordon	10.3	Annual Review
Dec 4, 2023	@Sarah Zwicker (Unlicensed)	10.2	Updated Security email from @peoplefluent.com to @ltgplc.com
May 16, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	10.1	Updated Password Administration section
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	10.0	Annual review + Logo change
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	9.9	Title change for VP InfoSec, Annual Review (no major changes noted)
Jun 15, 2021	@Sarah Zwicker (Unlicensed) & @Art Machado	9.8	Updated Scope and Purpose
Mar 10, 2021	@Sarah Zwicker (Unlicensed)	9.7	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	9.6	Reformatting, linked policies
Jan 26, 2021	@John Cole	9.5	Annual review
11/20/2020	John Cole	9.4	Changed owner