INFORMATION TECHNOLOGY

Source: The complete Information Technology policy and procedure section has been excerpted from the HR "Employee Handbook" located @ https://campus.dts.edu/staff/forms.shtml .

PURPOSE: The purpose of the Information Technology ("IT") department at Dallas Theological Seminary ("DTS") is to provide quality computer support and advice to meet computer system and telecommunication system needs at DTS. IT is responsible for the management of the central computer servers, the central campus telephone system, and all DTS-owned computer systems. Also, computer support for DTS employees, printer support, and computer hardware maintenance are managed by this department. IT coordinates the use of the computer systems on all campuses and seeks to ensure their effective, efficient, ethical, and secure use in support of DTS' mission.

IT POLICY TERMINOLOGY

All words and acronyms that are completely capitalized within the text of this document are defined under the section entitled: "IT Glossary."

IT POLICY PURPOSE

Though not exhaustive, the purpose of this policy is to outline the rules governing the EQUIPMENT, NETWORKS, USER DATA, SOFTWARE, and INTERNET at DTS by all USERS.

These rules are in place to protect the USERS and DTS. Inappropriate use exposes DTS and USERS to risks such as the misuse of personal information and financial assets, virus and spam attacks, the compromise of networked systems, denial of service attacks, and legal statutes.

DTS provides computing, telephone, and networking resources to students, faculty, staff, and others. Such access is a privilege granted by DTS to support the members of its ministry and mission as the DTS community works and learns in an environment supportive of education and service.

Supplemental expectations and codes of conduct regarding responsible behavior are contained in the complementary policies that are available from Student Services (for students), Academic Dean (for faculty), Human Resources (for all employees), and Business Services (for all others).

Individual departments and entities within DTS may define "conditions of use" for technology services under their control. These statements must be consistent with this overall IT policy but may provide additional detail, guidelines and restrictions. See the section entitled, "IT Policy Enforcement" for procedures concerning conflicting polices and interpretations of same.

Where the use of other networks (for example, the INTERNET) is involved, more restrictive policies and laws (US and other) governing such may in some cases take precedence over DTS' policies and by-laws. The USER is responsible to know and adhere to the standards and terms of use of such networks. DTS cannot be held liable for use of other networks. DTS cannot and will not extend any protection to you, the USER, should you violate the policies and laws of other networks.

Supplemental information about vendors, licensing agreements, policies (DTS and other) and laws (US and other) can be found at http://helpdesk.dts.edu, http://campus.dts.edu, or http://www.dts.edu. DTS does not warranty the accuracy or completeness of the supplemental information.

Use of DTS' owned and/or operated computers, telephones, computer networking, and any other technology resources owned or operated by DTS implies that you, the USER, agree to be governed by these policies as written and implemented. Your only recourse, if you do not agree to this IT Policy, is for you not to use the DTS RESOURCES.

IT POLICY SCOPE

This policy applies to all USERS as related to the use of DTS RESOURCES as defined under the section entitled, "IT Policy Glossary." This policy does not apply to any USER while they are not utilizing any DTS RESOURCES.

IT POLICY LIMITATIONS

Nothing contained in this policy is intended to modify or amend any other written agreement or policy, if any, that may currently be in effect between you, the USER, and DTS with regard to matters other than your use of the DTS RESOURCES unless these other policies or agreements reference the IT Policy. No USER has any inherent rights to any DTS RESOURCES. No rights are implicitly granted by DTS to the information contained herein or the information (or USER DATA) contained in or on any DTS RESOURCE. All rights are reserved. All standard disclaimers apply.

DTS may modify, suspend, discontinue, or restrict the use and availability of any portion of the DTS RESOURCES at any time, without notice or liability. All USERS may be monitored by DTS without any liability to DTS.

DTS may periodically modify this IT Policy, and any such modifications will be effective immediately upon posting. We suggest that you periodically check http://campus.dts.edu for the published IT Policy for the prevailing set of rules. If you do not agree to the IT Policy, you may not use any DTS RESOURCES.

Further policy limitations are stated under the section entitled: "IT Policy Disclaimer."

IT POLICY USAGE TERMINATION

Without limiting other possible remedies or methodologies, DTS may at any time and for any reason restrict or monitor access to DTS RESOURCES. DTS may issue a warning, temporarily suspend usage, unintentionally suspend or terminate usage without notice, restrict usage as needed, monitor usage as needed, indefinitely suspend usage or terminate usage and refuse to provide DTS RESOURCES to any USER:

1. If the USER violates any DTS policy;
2. If the USER does not agree to the current IT Policy at DTS;
3. If DTS believes that the USER may cause any liability for any USER or DTS;
4. If DTS has reason to believe that the USER'S behavior while using DTS RESOURCES is unethical or immoral;
5. If DTS determines you are not an authorized USER;
6. If DTS has been instructed to terminate usage by court order;
7. Or at any time or for any reason DTS warrants.

You, the USER, agree to indemnify and hold harmless DTS and (as applicable) all subsidiaries, affiliates, divisions, officers, directors, agents, volunteers, students, alumni, interns, and employees as a result of any form of usage termination that DTS determines is the best remedy in the interest of DTS, it's USERS, and its mission. See also the policy section entitled, "IT Policy Enforcement."

IT POLICY VIOLATION REPORTING

In general, reports about severe violations of this policy should be directed to the appropriate Vice President or as appropriate to the director of Human Resources. All USERS are obligated to notify the IT department about personally witnessed violations by sending confidential email to abuse@dts.edu.

IT SECUITY POLICY

Effective security is a team effort involving the pro-active participation and support of all DTS USERS. Security is the responsibility of all USERS. It is the responsibility of every USER to know these guidelines, and to conduct their activities accordingly. DTS reserves the right to audit USERS and DTS RESOURCES on a periodic or regular basis to ensure compliance of the IT policy.

The DTS REOURCES are intended solely for the communication, transmission, processing, and storage as it pertains to the mission of DTS. For security purposes and to ensure that the DTS RESOURCES remains available to all USERS, the IT department monitors network traffic to identify unauthorized attempts to upload or change information or to otherwise cause damage to DTS RESOURCES.

Unauthorized attempts to modify any information stored on DTS RESOURCES, to defeat or circumvent security features, or to utilize DTS RESOURCES for other than its intended purposes are prohibited and may result in criminal prosecution.

If monitoring reveals evidence of possible criminal activity, such evidence may be provided to law enforcement personnel. In addition, if you send us information about a threat or comments that constitute or might constitute a threat, or your comments contain information about criminal activities, we may provide that and associated information to law enforcement and/or other appropriate authorities.

IT Security Policy - Acceptable Use:
IT will make every reasonable effort to ensure that all use of DTS RESOURCES complies fully with applicable DTS policy statements, DTS bylaws, and appropriate laws (US and other).

1. Keep passwords and security codes secure and do not reveal your, the USER, access codes to anyone or any entity. This restriction includes but is not limited to access codes for computers, security codes for voice mail, website login credentials, personal identification numbers, and email passwords.
2. Authorized USERS are responsible for the security of their passwords, accounts and USER DATA that can be accessed based on the USER'S security clearance and authority. USERS should be familiar with the portion of the Risk Management Policy that governs USER DATA retention.
3. Privacy is very much related to security. Every USER is responsible to know and follow the IT Privacy Policy.
4. Use of DTS RESOURCES constitutes consent to security monitoring by DTS. USERS should remember that their use of DTS RESOURCES is not private. DTS audits, logs, and in other ways registers USER activities while accessing DTS RESOURCES.
5. Change your, the USER, password periodically to help prevent password theft and USER DATA misuse.
6. For the USERS or DTS' protection, DTS reserves the right to block INTERNET access as it relates to spam, viruses, pornography, gambling, instant messaging, voice-over-internet, disruptive technology, and for any other reason DTS determines degrades DTS RESOURCE security.
7. All EQUIPMENT should be secured by the USER via typical methods of logging-off or locking when the EQUIPMENT will be unattended. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the EQUIPMENT will be unattended. Do not assume others are protecting DTS RESOURCES.
8. USERS should take all necessary steps to prevent unauthorized access to DTS RESOURCES.
9. Every precaution should be made by USERS when using public computers or public networks to access DTS RESOURCES remotely.

10. Acceptable use of copyrighted material for educational purposes is authorized as governed by US federal copyright laws and international treaties.
11. Each authorized USER will maintain their own unique login credentials, associated with one USER and one USER only.
12. Every USER retains the rights of their personal USER DATA except where applicable and as described under "IT Security Policy - Unacceptable Use."

IT Security Policy - Unacceptable Use:
The following activities are, in general, unauthorized. Under no circumstances is a USER authorized to engage in any activity that is illegal under local, state, US federal law or international treaties while utilizing DTS RESOURCES.

The items listed below are by no means exhaustive, but are a reasonable attempt to provide the framework for USER activities which fall into the category of unacceptable use. Exceptions are noted for IT personnel under the section entitled, "IT Department Policy."

USERS may not:
1. Execute any form of DTS RESOURCE monitoring which will intercept data not intended for the USER'S EQUIPMENT, unless this activity is a part of the employee's normal job or duty while employed by DTS' IT department;
2. Reveal USER account password information to others or allow use of your account by others;
3. Circumvent USER authentication or the security of any DTS RESOURCE;
4. Use any program, script, command, utility, software, hardware, or application of any kind, with the intent to interfere with, or disable USERS' EQUIPMENT via any means;
5. Provide unauthorized information about, or lists of, USER DATA to unauthorized USERS;
6. Violate the rights of any person or organization protected by copyright, trade secret, 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 DTS or at DTS;
7. Abuse copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, audio files, video files, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DTS or the USER does not have an active license;
8. Export software or hardware, technical information, encryption software or technology, in violation of international or regional export control laws;
9. Intentionally introduce malicious SOFTWARE into or onto DTS RESOURCES (e.g., viruses, worms, trojan horses, ad-ware, spy-ware, etc.);
10. Use DTS RESOURCES to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws by any USER;
11. Make fraudulent offers of products, items, or services originating from any DTS account or DTS RESOURCE;
12. Make statements about warranty, expressly or implied using DTS RESOURCES unless it is a part of normal job duties;

13. Cause security breaches or disruptions of DTS RESOURCES;
14. Scan, decompile, reverse-engineer, interrogate, or in any other manner improperly search for USER DATA;
15. Store USER DATA such as social security numbers, driver's license numbers, dates of birth, donor records, medical records, payroll records, credit card numbers, debit card numbers, personal identification numbers ("PIN"), driver's license numbers, immigration numbers, or student records on EQUIPMENT that is portable or that can be easily removed from DTS property;
16. Transmit USER DATA via unsecured and non-encrypted methods such as fax, email, INTERNET, or instant messaging via wired or wireless means;
17. Participate in online auctions or bidding using registered DTS names or identification via any DTS RESOURCE unless part of the USER'S explicitly defined work related duties;
18. Make political statements using registered DTS names or identification via any DTS RESOURCE;
19. Intentionally access pornographic, sexually explicit, sexual images, or gambling web sites using any DTS RESOURCE;
20. Use DTS RESOURCES to engage in illegal, illicit, or pornographic behavior;
21. Seek information on, obtain copies of, or modify files, tapes, CDs, DVDs, or passwords that belong to other USERS or DTS;
22. Divulge USER DATA to which you have access concerning USERS without explicit authorization.
23. Maintain a login and password for communal use. Each USER must only have their own explicit, uniquely identifiable, and auditable login access for every authorized and accessible DTS RESOURCE.
24. Endorse any product or services, participate in any lobbying activity, or engage in any active political activity as a representative of a 503c organization using the DTS RESOURCES.
25. Intentionally develop or use any unauthorized mechanisms to alter, negate, or avoid financial charges levied by DTS for computing, printing, data processing services, electronic shopping carts, purchases, long distance calls and special phone services, tuition or fees, or any other DTS services while using any DTS RESOURCE.
26. Save any PASSWORD by using the "Remember my settings," "Remember my ID on this computer," or similar "Remember" options when automatically offered or manually set within the SOFTWARE options, properties, or comparable settings.

IT PRIVACY POLICY

The DTS is committed to protecting your privacy and will collect no personal information about you unless you, the USER, choose to provide that information to us or unless otherwise directed by this IT Policy or US laws. The IT Privacy Policy is a supplement to the DTS Privacy Policy and is not intended to usurp or countermand same.

DTS may use your, the USER, intranet or Internet identification to help DTS diagnose problems with DTS RESOURCES.

We do not sell names or information to anyone or any entity. Any name or address information you provide us with will be used to complete any requests you may wish us to process. We do not share this information with anyone or any entity except to the extent necessary in completing a transaction you authorized. Examples include but are not limited to: verification of credit card transactions, postal delivery systems, admissions processing, bank debits, student loans, insurance claims, US government processes and verifications.

DTS safeguards the security of the data you send us with physical, electronic, and managerial procedures. Likewise, we urge you to take every precaution to protect your personal data when you are on the INTERNET. Change your passwords often, using a combination of letters, numbers and symbols, and make sure you use a secure browser.

The DTS websites use industry-standard Secure Sockets Layer (SSL) encryption on all web pages where personal information is required. When entering personal information, we strongly recommend an SSL-enabled web browser. Web browsers developed after Internet Explorer 3 and Netscape 3 use SSL version 3. (For the best experience at the DTS web sites, DTS recommends using one of the following browsers or a more current version of same: Netscape 7.x, IE 6.x, or Fire Fox 1.5). This helps protect the confidentiality of your personal and credit card information while it is transmitted over the INTERNET. On some areas of DTS web sites, USERS do have the option to use a non-SSL connection. We do this for compatibility for older browsers.

When you enter credit card information on the DTS web sites, we do not store credit card numbers on the DTS RESOURCES. Credit card numbers are submitted to a credit card authorization service. This service provides DTS with credit card validation information only. We do not have access to your personal financial data.

IT MESSAGING POLICY

The pervasiveness of INTERNET MESSAGING is more and more obvious. Because of the manner that INTERNET MESSAGING and email in general are used, the proper use of MESSAGING requires the compliance of all DTS USERS. DTS reserves the right and in some cases may be legally obligated to record, log, and store all MESSAGING communications. The USER should assume that no MESSAGING is private. DTS allows the use of its MESSAGING addresses and retains the right to control the use of its MESSAGING addresses. DTS at its own choosing may add or revise MESSAGING disclaimers to any MESSAGES that are sent or received via DTS RESOURCES.

DTS' MESSAGING systems generally must be used only for DTS mission related activities. DTS does not warrant or guarantee the timely or accurate delivery of any messages, any electronic MESSAGING, any digital file, any digital image, or audio/video image transmitted over DTS RESOURCES by any USER, INTERNET provider or affiliated services.

IT Messaging Policy - Acceptable Personal Use:
Incidental personal use is permissible so long as:
1. It does not consume more than a trivial amount of DTS RESOURCES.

2. It does not interfere with any DTS mission related activities.

IT Messaging Policy - Acceptable Use:

1. DTS MESSAGING addresses and numbers may be used in a manner that adheres to DTS' mission.
2. Postings and communications using DTS email addresses, DTS INTERNET identification or DTS MESSAGING identification by any USER must contain a disclaimer if the USER is permitted to use DTS MESSAGING to post to news groups, blogs, discussion groups, chat rooms, or any similar methods of communication that uses DTS MESSAGING. The USER'S comments should contain a disclaimer stating that the opinions expressed are strictly the USER'S and not necessarily those of DTS, unless the postings are in the course of the USER'S explicit and approved DTS duties. The following is a disclaimer example: "The opinions expressed are my own and not necessarily those of DTS."
3. USERS may accept MESSAGE attachments but must use extreme caution when opening MESSAGE attachments received, MESSAGES may contain viruses, disruptive code that negatively impacts DTS RESOURCES, disruptive SOFTWARE, or surveillance SOFTWARE. Even if the sender is known by the USER, attachments should be opened with caution. Ask the question, "Am I expecting an attachment from the message's originator?"

IT Messaging Policy - Unacceptable Use:

DTS RESOURCES are not to be used as itemized below:

1. MESSAGING content in violation of faculty and staff employment handbooks or student conduct policies.
2. Using MESSAGING systems or networks for unauthorized commercial, for-profit or political activity.
3. Sending and receiving MESSAGING which violates local, state, or US federal laws.
4. Using MESSAGING that contains offensive materials that create a hostile working or learning environment.
5. The USER should never create either the appearance or the reality of inappropriate use of the MESSAGING systems, sites, and services.
6. USERS are forbidden to transmit MESSAGES that contain USER DATA.
7. USERS shall not participate in any and all online auctions or bidding processes using a DTS MESSAGING address unless this participation is explicitly described in the USER'S defined work related duties and responsibilities.
8. USERS may not reveal, market, sell, exchange, mass email, spam, phish, publish, copy, or counterfeit any DTS MESSAGING addresses or numbers.
9. USERS may not use VoIP (voice-over-IP) or any variation of same using DTS RESOURCES.
10. The DTS email system or the DTS MESSAGING systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. USERS who receive any emails with this content from any DTS USER should report the matter to the Director of Human Resources immediately.

IT Messaging Policy – Spam:

If you sent an email directly to a DTS mailbox and it was blocked, your e-mail may have been inadvertently captured by our spam filter. DTS RESOURCES uses measures that are generally effective against blocking spam. Any approach to filtering, however, results in some legitimate email being lost. DTS continues to monitor the situation to keep spam at a manageable level and minimize the loss of legitimate email.

No USER is permitted to use any DTS RESOURCES to SPAM any other user or the Internet.

IT INTERNET POLICY

INTERNET access generally must be used only for DTS mission related activities. Incidental personal use is permissible so long as:

1. It does not consume more than a trivial amount of computing and networking resources.
2. It does not interfere with any DTS mission related activities.

IT Internet Policy - Unacceptable Use:

The INTERNET shall not to be used as described:

1. The USER may not access the INTERNET content in violation of faculty and staff employment handbooks or student conduct policies is strictly prohibited.
2. The USER may not access the INTERNET for unauthorized commercial or for-profit activity.
3. The USER may not access the INTERNET in a manner that violates local, state, US federal, or international treaties.
4. The USER may not access the INTERNET to access offensive materials that creates a hostile working or learning environment.
5. The USER should never create either the appearance or the reality of inappropriate use of the INTERNET.
6. The USER may not use the INTERNET to transmit USER DATA except where explicitly permitted by DTS policies.
7. The INTERNET shall not be used for immoral and illicit behavior.
8. The USER may not cause security breaches or DTS RESOURCE disruptions while using the INTERNET.
9. The USER may not scan, decompile, reverse-engineer, interrogate, or in any other manner improperly search for USER DATA while using the INTERNET.
10. The USER may not store USER DATA such as social security numbers, driver's license numbers, dates of birth, donor records, medical records, payroll records, credit card numbers, debit card numbers, personal identification numbers ("PIN"), driver's license numbers, immigration numbers, or student records on the INTERNET or allow it to be accessible from the INTERNET unless explicitly permitted by DTS policies.
11. The USER may not transmit USER DATA via an unsecured or non-encrypted manner over the INTERNET.
12. The USER may not participate in online auctions or bidding using registered DTS names or identification via the INTERNET unless part of the USER'S explicitly defined work related duties.

13. Make political statements using any registered DTS names, addresses, or identification via the INTERNET.
14. The USER may not intentionally access pornographic, sexually explicit, sexual images, or gambling web sites using the INTERNET.
15. The USER may not use the INTERNET to engage in illegal, illicit, or pornographic behavior;
16. The USER may not seek information on, obtain copies of, or modify files, tapes, CDs, DVDs, or passwords that belong to USERS, persons, or entities on the INTERNET that do not belong to the USER;
17. A USER may not divulge other USER'S DATA on the INTERNET without explicit authorization.

IT Internet Policy - General Guidelines:

1. Regardless of the rationale, INTERNET passwords must never be shared or revealed to anyone or any entity.
2. The USER should regularly change passwords to help prevent password theft, USER DATA theft, or DTS RESOURCE misuse.
3. DTS will regularly monitor and log the USERS attempts to access websites and information on the INTERNET.
4. DTS will restrict access to INTERNET websites and services when it determines the restrictions are in best interest of DTS, its mission, and the USERS.

IT SOFTWARE POLICY

The IT department will make every reasonable effort to ensure that all SOFTWARE residing on all DTS RESOURCES complies fully with applicable SOFTWARE licensing agreements and US laws. In addition, any PERSONAL EQUIPMENT that is authorized to connect to any DTS RESOURCE must adhere to this same DTS SOFTWARE policy.

IT Software Policy – Acceptable Use:

The USER shall ensure compliance with the SOFTWARE usage and licensing policies by:

1. Acquiring SOFTWARE in accordance with the DTS Purchasing department's policies and all United States federal, state, and local laws;
2. Maintaining valid purchase records for all SOFTWARE installed on all DTS RESOURCES;
3. Adhering to the manufacturer's End User License Agreements ("EULA").
4. DTS provided SOFTWARE may be installed by USERS on PERSONAL EQUIPMENT if the SOFTWARE license permits.

The EMPLOYEE in addition to USER compliance shall also:

1. Acquire SOFTWARE in accordance with the DTS Purchasing department's policies;
2. Be cognizant of the IT supported SOFTWARE itemized at http://helpdesk.dts.edu;
3. Upgrade or add SOFTWARE as instructed by the IT department.
4. Contract all SOFTWARE licenses and agreements through Business Services.
5. Purchase only approved SOFTWARE.

IT Software Policy – Unacceptable Use

1. No USER may knowingly break local, state, or federal laws using SOFTWARE on DTS RESOURCES or aided by DTS RESOURCES.
2. No USER may install SOFTWARE that will seek to subvert DTS RESOURCE security.
3. No USER may install SOFTWARE that will disrupt DTS RESOURCES or impact any privacy rights.
4. No USER may accept any SOFTWARE license, contract, end-user license agreement, or usage agreement that has not been explicitly approved by the Business Services.
5. No USER may purchase, install or connect any SOFTWARE that has not been explicitly permitted by this IT Policy or approved using the SOFTWARE usage variance forms and procedures outlined at http://helpdesk.dts.edu.

IT EQUIPMENT POLICY

The IT department will make every reasonable effort to ensure that all EQUIPMENT residing on or connected to all DTS RESOURCES complies fully with applicable policies and procedures, agreements and US laws. In addition, any PERSONAL EQUIPMENT that is authorized to connect to any DTS RESOURCE must adhere to the DTS EQUIPMENT policy and the IT Policy.

IT Equipment Policy – Acceptable use:

1. Install only EQUIPMENT permitted by the current IT Policy and procedures.
2. Employees must only purchase approved EQUIPMENT through approved DTS departments and vendors.
3. DTS provided EQUIPMENT may be installed or attached by USERS on/to PERSONAL EQUIPMENT if explicitly permitted by IT procedures or approved IT variance forms.
4. USERS may only connect PERSONAL EQUIPMENT to DTS RESOURCES if connected in accordance with the current IT Policy and all other DTS policies. Plus, the USER must assume all liability for misuse, damage, and restitution.

IT Equipment Policy – Unacceptable Use:

1. No USER may knowingly break local, state, or federal laws using EQUIPMENT connected to DTS RESOURCES or aided by DTS RESOURCES.
2. No USER may install EQUIPMENT that will seek to subvert DTS RESOURCE security.
3. No USER may install EQUIPMENT that will disrupt DTS RESOURCES or impact any privacy rights.
4. No USER may purchase, install or connect any EQUIPMENT that has not been explicitly permitted by this IT Policy or approved using the EQUIPMENT usage variance forms and procedures outlined at http://helpdesk.dts.edu.
5. No USER may use any DTS EQUIPMENT or any DTS RESOURCES for commercial, for-profit, or public enterprises or activities unless explicitly allowed in other DTS policies, agreements or written and approved contracts.

IT POLICY – APPROPRIATE AND RESPONSIBLE USE:

1. Because information contained on portable EQUIPMENT is especially vulnerable, special care should be exercised by all USERS.
2. All EQUIPMENT should be protected by current virus protection. This is especially true if the USER attaches the EQUIPMENT to DTS RESOURCES.
3. No reputable Internet organization will send an unsolicited request for USER DATA. Always verify MESSAGING requests of this nature before responding.
4. All DTS and PERSONAL RESOURCES must be disposed of properly. All DTS USER DATA must be erased so it is no longer readable or recoverable. This applies when the USER donates, sells, trashes, and otherwise disposes of any EQUIPMENT that may have contained or contains DTS USER DATA. DTS suggests that these same procedures are applied whenever EQUIPMENT requires disposal whether or not the EQUIPMENT knowingly contained or contains DTS USER DATA. All EQUIPMENT should be trashed in accordance to local, state, and US federal regulations.
5. No USER may assume another person's or USER'S identity or role through deception or without proper authorization. You may not communicate or act under the guise, name, identification, MESSAGING address, signature, or indicia of another person without proper authorization, nor may you communicate under the rubric of an organization, entity, or unit that you do not have the authority to represent.
6. USERS are reminded that the storage and transmission of electronic materials can be disrupted by hardware and software failure as well as by hacking or other unauthorized access. It is the USER'S responsibility to back up their materials except for instances where DTS specifically commits to provide backups. Likewise, USERS are cautioned about storing or transmitting material which they view as confidential.
7. Only access DTS USER DATA from EQUIPMENT you know is secure.
8. DTS strongly suggests never using a "cookie" to store a password.
9. Any public RESOURCE, PERSONAL EQUIPMENT, DTS EQUIPMENT, or DTS RESOURCE you use may be subpoenaed during a legal investigation.
10. The telephone in many cases is no longer a distinct technology. Rules, policies, and regulations now consider the telephone as IT EQUIPMENT and are therefore governed accordingly.
11. Technology changes are quick and often. The USER is obligated to regularly review current IT Policies at DTS. The current policies will be posted on http://campus.dts.edu.

IT POLICY – USER TERMINATION (VOLUNTARILY AND INVOLUNTARILY):

This policy applies to those USERS who resign, quit, graduate, are fired, fulfill their contract, void their contract, or for any other reason terminate a USER relationship with DTS. These ex-USERS must remove within 72 hours all previously licensed and authorized DTS RESOURCES from their PERSONAL EQUIPMENT. This includes but is not limited to SOFTWARE, computer peripherals, USER DATA, email addresses, firmware, passwords and pass codes, and other DTS RESOURCES that have been loaned to the USER for temporary use. DTS will ask for confirmation and may ask for verification of ex-USER'S compliance.

IT POLICY GLOSSARY:

These terms and definitions are not exhaustive but the words and acronyms have been created for the purposes of clarifying the IT Policy text, its meaning, and the intent, as it relates to using DTS RESOURCES.

Term	Definition
DATA	Such as but not limited to: social security numbers, driver's license numbers, dates of birth, donor records, medical records, payroll records, credit card numbers, debit card numbers, personal identification numbers ("PIN"), driver's license numbers, immigration numbers, student records, voice mail, and email. This type of information is also considered individually identifiable. DTS maintains information obtained while monitoring DTS RESOURCES. This includes but is not limited to time of day and date, access logs, logs of web sites accessed, personal credentials used, and messaging credentials while using DTS RESOURCES.
DTS	Dallas Theological Seminary, 3909 Swiss Ave., Dallas Texas, 75204 plus all affiliated ministries and campuses as described in all other related Dallas Theological Seminary policy statements and by-laws. All registered and customary names plus logos are owned, registered, and copyrighted by the organization known as Dallas Theological Seminary.
EMPLOYEE	Any person who is considered a staff or faculty member by the DTS Human Resource department is an employee.
EQUIPMENT	This policy applies to all DTS and PERSONAL technological hardware, storage media, removable media, and firmware that is owned, used, rented, and leased. EQUIPMENT includes but is not limited to personal computers, workstations, laptops, servers, computer network hubs, phone systems, software, PDA's, cell phones, data, memory cards, tapes, recording devices, CDs, DVDs, and any other device that contains a micro processor or electronic storage capacity (a.k.a. equipment, hardware).
INTERNET	The universal network that allows EQUIPMENT to talk to other EQUIPMENT in words, text, graphics, light pulses, binary data, audio tones, and sounds, anywhere in the world or solar system via wired and wireless NETWORKS (a.k.a. Internet, the web, world wide web).
IT	The Information Technology department at Dallas Theological Seminary.
MESSAGING	Includes but is not limited to: email messages ("email"), instant messaging ("IM"), digitally transmitted video images, digitally transmitted audio files, transmitted files, wired telephone communications, wireless telephone communications ("cell", "PDA"), and fax communications (a.k.a. Messaging, messaging,

	MESSAGES, messages).
NETWORK	The attachment of any EQUIPMENT via a physical ("wired") or wireless connection(s) (a.k.a. NETWORKS).
PASSWORD	A series of characters that enables someone to access a file, personal data, a computer, a bank account, a web site, voicemail or a computer program. The password should be a combination of characters that would be difficult to guess. Good passwords: look like random characters, contain at least 6 characters, are easy to remember, are not written on a post-it note, and are a secret. (a.k.a. password, passwords, PIN, security code, key code, access code)
PERSONAL	A person who owns, leases, rents, controls, is liable for, has contractually agreed to, or operates the RESOURCES (a.k.a. personal, personally).
RESOURCE	Any combination of EQUIPMENT, INTERNET, NETWORKS, SOFTWARE, TBA, and USER DATA (a.k.a. RESOURCES, SYSTEMS, systems)
SOFTWARE	The digital programs, applications, operating systems, firmware, sound and video files, scripts, fonts, command and executable files, and binary code that must be loaded onto EQUIPMENT to function as designed (a.k.a. software).
SPAM	Typically defined as Unsolicited Bulk Email (UBE). Another synonym for email spam is UCE, Unsolicited commercial email promoting a commercial service or product. This is the most common type of SPAM.
SUBVERSIVE EQUIPMENT	Any *EQUIPMENT not owned or explicitly approved by the IT department* (e.g., hub, switch, router, antennae, alternative cabling, computers, surveillance devices, etc) intended to supplant DTS' NETWORKS or RESOURCES for the purpose of providing connectivity to multiple *computers*, peripherals or bypassing the DTS policies and security.
TBA	To Be Announced – any technology that was not imagined, designed, invented, or implemented at the time this policy was written and approved.
USER	Any person or entity that is explicitly allowed to use, rent, lease, borrow, repair, maintain, or support any EQUIPMENT owned, rented, borrowed, or leased by DTS. This policy applies to employees, students, contractors, consultants, temporaries, interns, volunteers, trustees, board members, and other workers at DTS, including all personnel affiliated with third parties, contractors, and vendors if given explicit contractual rights of limited access to DTS RESOURCES. All USERS must be 18 years or older (a.k.a. USERS, USER'S, USERS', user, end-user).

IT POLICY ENFORCEMENT:

DTS characterizes as unacceptable, and may be just cause for taking disciplinary action up to and including discharge, dismissal, and/or legal action, any activity through which a USER:

1. Intentionally violates DTS or third party copyrights, license agreements, or other contracts;
2. Purposely interferes with the intended and designed use of the DTS RESOURCES;
3. Seeks to gain or gains unauthorized access to DTS RESOURCES;
4. Without explicit authorization: destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of DTS RESOURCES; or
5. Wrongfully transmits or otherwise reveals USER DATA.

Any USER found to have violated this IT Policy may be subject to disciplinary action. The Executive Director of Communications and Information Technology ("CIT"), the USER'S VP in-charge, and the Director of Human Resources will be responsible for interpretation of DTS policy and the severity of any violation when implementing the following procedures:

Level 1 - Minor problems: IT notifies the USER of the problem and requests that the violation stop. If the violation ceases no further action is taken. Example: a USER gives their password to another person. IT notifies the USER that this is a violation of the IT Policy and requires that the USER changes their password. The USER complies and no further action is taken. The USER'S immediate supervisor is notified.

Level 2 - Serious or repeated problems: The IT staff and department head will consult with the Executive Director of CIT before taking any action. If the Director of CIT is unavailable and the problem is time-critical, consultation should be made with the appropriate Vice President. Any action taken by IT will be under the guidance of the appropriate Vice President, the Executive Director of CIT, and the Director of Human Resources, as appropriate. A letter describing the action and the sanction will be sent to the appropriate Vice President and HR to be put in the employee's personnel file. Example: a USER uses DTS RESOURCES to advertise and distribute pirated materials on the INTERNET. IT notifies the USER that this is a violation of the IT Policy (and US laws) and requires the USER to desist. The USER agrees to have a letter describing the action and the sanction recorded in their personnel file.

Level 3 — Major problems: The Executive Director of CIT, HR, and the appropriate Vice President should be notified immediately. If a law is broken or a threat of bodily harm is involved, others may be immediately notified as circumstances require. Any necessary action will be taken by the appropriate officer(s). Example: IT obtains notification that someone has received a threatening email from a USER. Upon investigation IT verifies that the email was indeed sent by a USER. IT secures the audit logs. IT suspends USER access to DTS RESOURCES. The relevant authorities are notified.

Disciplinary enforcement as documented in this policy does not limit DTS' options. DTS may terminate for any reason.

IT DEPARTMENT POLICY:

Each IT staff member must read, accept, and sign the document entitled: "IT Policy Integrity Statement" as part of their employment conditions. This document includes but is not limited to the requirement that each IT staff member must maintain strict confidentiality with regard to all USER DATA obtained in the normal course of business. A copy of the signed "IT Policy Integrity Statement" will become part of the IT staff member's permanent personnel records and a copy may be retained by the IT staff person if they so wish.

The IT staff will not share any USER DATA with any third parties, except as authorized by and required by DTS policies.

For security purposes, authorized individuals within the IT department at DTS may monitor DTS RESOURCES and USERS at any time. Authorized IT staff may be exempted from a portion of the unacceptable IT policies and restrictions during the course of their legitimate job responsibilities (e.g., IT staff may have a need to disable DTS EQUIPMENT to prevent a virus attack from disrupting production services). This exemption is not a "blank check" for IT personnel to break DTS policies or US laws, only to provide a "safe harbor" for the typical IT responsibilities in an academic and a corporate work environment. For this policy statement, DTS assumes: "A safe harbor is a provision of a statue or a regulation that reduces or eliminates a party's liability under the law, on the condition that the party performed its actions in good faith. Legislators include safe-harbor provisions to protect legitimate or excusable violations."
Source: http://en.wikipedia.org/wiki/Safe_Harbor

IT staff shall not ask you, the USER, for your passwords. For this reason, you should inform the DTS Campus Police if anyone ever contacts you and asks you for your login credentials.

IT department staff must report all violations of the IT Policy. They will report violations as prescribed under in the DTS "Employee Policy Handbook" which includes but is not limited to the IT Policy section entitled: "IT Policy Enforcement."

IT POLICY REFERENCES AND SOURCES:

1. Several portions of the IT Policy text is sourced from US Federal documents and policies available through the internet which are covered under US Copyright law Title 17, Chapter 1 and Section 105: "Copyright protection under this title is not available for any work of the United States Government…"
2. Explicit permissions are stated at https://www.cia.gov/cia/notices.html#priv for test located at www.cia.gov:
   "Unless a copyright is indicated, information on the Central Intelligence Agency Web site is in the public domain and may be reproduced, published or otherwise used without the Central Intelligence Agency's permission. We request only that the Central Intelligence Agency be cited as the source of the information and that any photo credits or bylines be similarly credited to the photographer or author or Central Intelligence Agency, as appropriate…"

3. Some portions of the IT Policy are used based on the expressed written permission of the DIT at Multnomah Bible College and Biblical Seminary (http://multnomah.edu).
4. Sections of this IT Policy are used by the expressed permission from SANS (SysAdmin, Audit, Network, Security) Institute (http://www.sans.org/resources/policies/).
5. A few policies are excerpted graciously provided by Reed College, Portland, Oregon per explicit permission from the CTO (http://www.reed.educis/policies).
6. Documents provided by http://en.wikipedia.org: Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

IT POLICY - DISCLAIMER:

The DTS RESOURCES are provided "as is" without warranty of any kind. DTS makes no claims as to the fitness of the DTS RESOURCES. DTS is not liable for any consequential damages related to DTS RESOURCES. The USER assumes all liability when connecting to DTS RESOURCES and using PERSONAL EQUIPMENT on properties owned and operated by DTS. Opinions or statements expressed on DTS SITES are not necessarily the opinions of Dallas Theological Seminary. DTS neither supports nor endorses any vendor, OEM, brand name, registered name, author, publisher, ministry, or services: referenced, used, listed, posted, installed, or licensed by DTS.

Source: The complete Information Technology policy and procedure section has been excerpted from the HR "Employee Handbook" located @ https://campus.dts.edu/staff/forms.shtml .

Revision date: 2006