Subject:	Information Technology Acceptable Use

516.1 Purpose

To establish guidelines and expectations for the acceptable use of information technology resources belonging to the Office of the Commissioner of Technical Education.

516.2 Approval

UCAT Board of Trustees approval: May 18, 2017.

516.3 References

UCAT Policy 507, Personal Conduct
UCAT Policy 525, Evaluation, Corrective Action, and Termination of Staff Personnel
UCA 76-10-1204.5, Reporting of Child Pornography by a Computer Technician

516.4 Definitions

4.1 Information Technology ("IT") Resource: A resource used for electronic storage, processing, or transmitting of any data or information, as well as the UCAT data or information itself. This definition includes but is not limited to: electronic mail, voice mail, local databases, externally accessed databases, software, computers and tablets, servers, removeable file storage, digital recordings, photographs, digitized information, student and institutional data, etc.

4.2 User: Any person who accesses and uses UCAT IT resources, including members of the UCAT staff, contractors, consultants, interns, temporary employees, etc.

4.3 IT Resource Administrators: The UCAT staff members designated by the Commissioner of Technical Education, who have policy level responsibility for determining what IT resources will be stored, who will have access thereto, what security and privacy risks are acceptable, and what measures will be taken to prevent the loss of information technology resources.

4.4 Private Sensitive Information: Private information that identifies or describes an individual (information owner), including but not limited to his or her name, Social Security Number, date of birth, and financial matters. Access to such data is governed by state and federal law, both in terms of protection of the data and requirements for disclosing the data to the individual to whom it pertains. Private sensitive information does not include "public information" as defined by the Utah Government Records Access and Management Act (GRAMA), or in the case of student records, "directory information" as defined by the Family Education Rights and Privacy Act (FERPA).

4.5 Confidential Information: Any information classified as confidential by the Commissioner of Technical Education or the cognizant associate or assistant commissioner.

Subject:	Information Technology Acceptable Use

516.5 Use of Office-owned Information Technology Resources

5.1 Official Business: Employees of the Office of the Commissioner of Technical Education are expected to use office-owned information technology ("IT") resources (including hardware, software, access to the internet, etc.) primarily for official business in connection to their job responsibilities, and not for personal use or entertainment. Staff members shall spend on-duty time (not including periodic or lunch breaks) on official business in connection to their jobs and not on personal affairs or entertainment. This expectation is qualified by normal allowance for emergencies that may arise, and for reasonable socializing that facilitates effective working relationships.

5.2 Office Breaks, Travel, or at Home: During break time or in the case of portable IT resources used while traveling or at home, UCAT policy does not prohibit limited personal use of IT resources, subject to the provisions below. "Limited" is to be interpreted literally, meaning a very small portion of the total use of IT resources.

5.2.1 Allowable Limited Personal Use: Limited personal use may include:

(a) Using an office phone on occasion to make necessary calls;

(b) Faxing an important document if necessary;

(c) Accessing the Internet for reasonable and appropriate personal use, for educational or research projects, to retrieve news stories or other information of general interest, to participate in professional or civic organizations, or to perform nonprofit or community service; or

(d) Using email to send or receive occasional brief messages to or from personal contacts.

5.2.2 Prohibited Limited Personal Use: Limited personal use of office-owned IT resources shall not:

(a) Directly or indirectly interfere with UCAT operations or IT resources;

(b) Compromise the security or reputation of UCAT;

(c) Burden UCAT with noticeable incremental cost;

(d) Infringe the copyright or other intellectual property rights of third parties; or

(e) Involve any activity prohibited under 516.15 or by generally accepted standards of computer ethics and etiquette.

5.2.3 Staff Liability for Unauthorized and Personal Use: Staff members shall exercise reasonable precautions in caring for any IT resources authorized for use

off premises, and are personally responsible for any damage resulting from personal use or use by unauthorized persons.

5.3 Security and Confidentiality Agreements: All UCAT employees shall sign a security and confidentiality agreement and must acknowledge in writing that they have read, understand, and agree to the terms contained in Policy 516, Information Technology Acceptable Use.

516.6 User Authentication

Access to UCAT IT resources must be authenticated using a PIN at a minimum, and a user ID and password when available. Users are responsible for the confidentiality and selection of passwords to ensure that unauthorized use of their UCAT user accounts does not occur.

6.1 Password Requirements

6.1.1 Individual user-IDs and passwords shall not be shared. No employee, including IT staff and an employee's supervisor, shall request another person's password(s).

6.1.2 User passwords should not be written down.

6.1.3 Passwords used on UCAT IT resources should not be used on non-UCAT IT resources.

6.1.4 Passwords should be changed regularly, even for applications that do not systematically require the change. When changing passwords, users should not reuse passwords that have previously been used for that specific IT resource.

6.1.5 Wherever possible, passwords should be sufficiently complex to minimize the potential for unauthorized access to UCAT IT resources. Care should be taken to include a mix of upper and lower-case letters, numbers, and special characters/symbols in all passwords.

6.1.6 Wherever possible, two-factor authentication is recommended.

6.2 Use of Third-party Password Management Services: UCAT employees are allowed to use third party password management services (e.g., LastPass, etc.), but must ensure that corresponding login credentials are of sufficient length and complexity to minimize the potential for unauthorized access to UCAT IT resources. All password requirements described in 516.6.1 shall apply to passwords for third-party password management services.

516.7 Internet Use

Subject:	Information Technology Acceptable Use

7.1 Internet Access and Use: Staff members are expected to exercise sound judgment in limiting their use of internet access to official business-related purposes during normal business hours. Any personal uses of office-provided internet capacity must be limited to breaks, lunch hour, or other off-duty time, and must be in keeping with standards of ethical behavior. IT resource administrators are instructed to monitor and periodically check the websites addressed using office internet access.

7.2 Downloaded Materials: Staff members must take care when downloading any materials from the internet, verifying the authenticity of material publishers and ensuring the security of UCAT IT resources. Staff members must not download any items with unrecognizable file extensions (e.g., .exe, .scr, .pif, .cmd, cpl, and .hta.) or from unverifiable sources.

7.3 Social Computing: UCAT employees are discouraged from publicly discussing work-related matters, regardless of their level of confidentiality and regardless of whether the employee is on company or personal time, outside of appropriate work channels, including through social media, online chat rooms or forums, personal blogs, etc. An employee engaging in these and other like mediums must:

7.3.1 Make it clear that the views expressed are the employee's alone and do not necessarily represent the views of UCAT;

7.3.2 Respect UCAT's confidentiality and proprietary information;

7.3.3 Ask his or her manager if there are any questions about what is appropriate to include in a social media or blog post, chat room or forum comment, etc.;

7.3.4 Be respectful to UCAT and its employees, customers, partners, and competitors;

7.3.5 Understand and comply when UCAT asks that topics not be discussed for confidentiality or legal compliance reasons; and

7.3.6 Ensure that social media activities, blogging, etc. do not interfere with UCAT work commitments.

516.8 Electronic Messaging System

8.1 Use of the Messaging System: The UCAT messaging system consisting of email/calendaring client software, email/calendaring servers, and supporting infrastructure is the property of UCAT and shall be used for legitimate UCAT business purposes. Users are permitted access to the messaging system to assist them in performing their responsibilities within UCAT. Use of the messaging system is a privilege that can be revoked at any time.

8.2 Users Responsible for Messages: Users are responsible for any messages sent or forwarded from their email account. Users shall take care upon receiving any message from an unknown person or website, and shall not select any hyperlinks or open any

attachments from unfamiliar sources or with unfamiliar file extensions (e.g., .exe, .scr, .pif, .cmd, cpl, and .hta.).

8.3 **Account Management:** IT resource administrators have primary responsibility for the UCAT messaging system. Accounts are available only to current UCAT staff, excepting recently-separated staff subject to the provisions of 516.18.2. Special consideration may be made for outside affiliates and consultants, and must be approved in writing by the Commissioner of Technical Education.

8.3.1 No user shall be allowed more than one mailbox in the messaging system.

8.3.2 Messaging system user IDs must be unique and in the form of a UCAT ID as issued by UCAT. The canonical email address for a user will be based on the messaging system user ID. Exceptions shall be allowed for work group resources (conference rooms, IT resources, and generic work group email addresses).

8.3.3 Users are responsible for safeguarding their passwords. Individual passwords must not be printed, stored online, or given to others (including family members).

8.3.4 The automatic forwarding of email to non-UCAT addresses is prohibited.

8.3.5 Unsolicited email (spam) and offensive external messages are to be deleted. Users should not respond to unsolicited e-mails, even to request removal from the mailing list.

8.4 **Delegated (Proxy) Access:** A user may grant delegated (proxy) access to another user in the email system. Requests for delegated (proxy) access must be approved in writing by the user whose account will be accessed. Individuals who request and receive access to another person's email shall not receive permission to directly access the email account, but will be allowed to choose email messages they would like printed or forwarded to them that directly relate to the issue(s) described in their request.

8.5 **Distribution or Storage of Prohibited Materials:** Email may not be used for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (i.e., viruses), or any other unauthorized use.

8.6 **Waste of Messaging System Resources:** Users may not deliberately perform acts that waste messaging system resources or unfairly monopolize resources to the exclusion of others. These acts include but are not limited to mass mailings, chain letters, or otherwise creating unnecessary network traffic. IT resource administrators, upon consultation with the Commissioner of Technical Education, reserve the right to disable mailboxes that are creating system-wide problems.

8.6.1 Users may not initiate or forward chain messages. Chain messages are defined as messages sent to a number of people asking each recipient to send copies of the same request to a number of other recipients.

8.6.2 Mass email is a message that is sent to a large number of recipients. All mass email must be approved in writing by the Commissioner of Technical Education or his or her designee before dissemination.

8.7 **Personal Use:** Limited personal use is allowed so long as it does not interfere with the operation of the email system and does not provide an added burden for UCAT messaging system administration.

8.8 **Sensitive Data:** Users shall not send email containing private sensitive or confidential information without proper data security protocols (i.e., encryption). Examples include but are not limited to FERPA and/or HIPPA-protected student information, login credentials, etc.

8.9 **E-Mail Access on Mobile Devices:** Users are permitted to access their UCAT email accounts through mobile communication devices, in addition to an applicable mail client's web interface. Standard IT support shall be provided for mobile device integration.

8.10 **Mail Retention and Backup:** Email users and those in possession of UCAT records in the form of electronic mail are cautioned to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid free paper or backed-up portable document formats (.pdf). Users shall back up and retain emailed messages in accordance with established backup and retention schedules.

8.11 **Monitoring:** All electronic messages transmitted on UCAT IT resources are subject to appropriate and periodic monitoring by IT resource administrators, as set forth in 516.16.

516.9 Telephone Use

9.1 **Use of Telephone Systems:** UCAT telephone systems and equipment are provided for the conduct of official business. Use of these facilities for personal business shall be kept to a minimum. Usage reports for all UCAT phones may be monitored for abnormally high usage volumes. Office telephone numbers shall not be formally published in connection to personal business. Office phone numbers should not be given out for incoming personal calls. These phone numbers are strictly for the use of UCAT clients, or prospective clients, to be used when contacting UCAT regarding official business.

9.2 **Long Distance and Toll Calls:** Long distance and other toll calls for personal use made through the UCAT telephone system should be charged to an individual's personal calling card. If this is not possible, a record of such calls made at UCAT expense must be kept and repayment must be made upon receipt of the telephone bill. IT resource

administrators and the Assistant Commissioner for Planning, Finance, and Facilities are responsible to prevent abuse and ensure that repayment is made. Personal collect calls shall not be accepted.

9.3 No Cellular Use while Operating a Motor Vehicle: Employees shall not use cellular telephones to conduct UCAT business while operating a motor vehicle.

516.10 Shared File Space

Users shall treat institutional data and files as confidential unless otherwise noted pursuant to state or federal statute, regulation, law, or Board of Trustees policy. Users shall not access files or documents in a shared file space (e.g., file closets, shared computer drives or email accounts, Microsoft SharePoint, etc.) without proper authorization or unless pursuant to routine system administration. With authorization, users shall access and use information only in a manner consistent with their job function(s). Users are responsible for safeguarding the integrity and confidentiality of all information to which they have access, and shall not store personal sensitive or confidential information on an IT resource unless appropriate safeguards are in place. Users shall not use external, non-UCAT IT resources to access UCAT IT resources without prior written approval, and shall not attempt to circumvent access or accounting controls in place.

516.11 Wireless and Remote Access

Office employees are permitted to occasionally access UCAT IT resources remotely, though care should be taken such that remote access does not become a habit. UCAT employees are expected to complete their work at the office via normal IT resource channels. Remote access users: (1) shall access the UCAT network only through approved channels; (2) are responsible for adhering to all UCAT policies while accessing the system; (3) shall protect UCAT information and assets while accessing the UCAT network; (4) shall not connect to multiple networks at the same time without prior IT resource administrator approval; and (5) shall not download private sensitive or confidential information to non-UCAT systems, including home computers, personal storage drives, and mobile communication devices.

516.12 Hardware

12.1 Inventory Control: An IT resource administrator, in consultation with the Assistant Commissioner for Planning, Finance, and Facilities, shall maintain an inventory of all physical IT resources purchased using UCAT funds.

12.2 Provision of IT Resources to Staff Members: Each user shall be provided physical, UCAT-owned IT resources with which to fulfill his or her job responsibilities. An IT resource administrator shall document each physical IT asset provided to a user. Upon provision of physical IT resources to a user, responsibility for the physical security of the resources shall rest upon the user. Users shall be held liable for lost or damaged hardware due to negligence or noncompliance with this policy. Unused UCAT-owned hardware in the possession of a user shall be returned to an IT resource administrator to protect against future liability.

12.3 Prohibited Activities: Users shall not install, reconfigure, or remove any hardware from UCAT IT resources without written authorization from an IT resource administrator. Users also shall not connect non-UCAT hardware directly to the UCAT network or UCAT IT resources. Exceptions shall be allowed for personal mobile phone access to wireless internet for acceptable use as described in 516.5.1-2.

12.4 Physical Security: Users are responsible for assuring that all electronic information, hard copy information, and hardware devices in their possession are physically protected at all times. IT resources containing private sensitive or confidential information shall never be left unattended without first securing physical access thereto.

12.4.1 Hardware containing private sensitive or confidential information, including CDs, flash or external drives, tablets, etc., must be kept in locked drawers, filing cabinets, or other secure places when not in use or when the work area is unattended.

12.4.2 Users shall not remove hardware containing private sensitive or confidential information from UCAT premises without the cognizant associate or assistant commissioner's approval. All transport activities shall be controlled and documented.

12.4.3 Users assigned to offices with locks shall lock their doors at the end of the workday.

12.4.4 Workstations, servers, mobile IT resources, and other computing devices shall be locked when left unattended.

12.4.5 Hardware found unattended or in inappropriate areas shall be returned to the owner, if known, or removed and securely stored until the owner is found or identified.

12.4.6 No staff member, contractor, or visitor shall compromise or evade physical restriction of access to the UCAT building or work areas.

516.13 Software

13.1 Authorization and Installation of Software: Software installed on UCAT IT resources shall be owned by the office and installed by an IT resource administrator or his or her designee. Installation of personal copies of software (e.g., video games, movie players, etc.) or installation of software by other staff members is prohibited unless written consent is granted by an IT resource administrator. This policy is intended to ensure compliance with software licensing obligations, safeguard against avoidable intrusion of computer viruses/malware, and avoid unnecessary overloading of memory and hard disc storage capacity of office-owned IT resources. Need for specialized software packages (apart from office-wide standard software modules) must be verified in writing by the cognizant

associate or assistant commissioner, charged to the applicable cost center budget, and installed by an IT resource administrator or his or her designee.

13.2 Downloading Software: Persons with internet access on office-owned IT resources may download documents related to their official duties, but are prohibited from downloading any software without first checking with an IT resource administrator to ensure both compliance with licensing requirements and protection against interference with other installed software.

13.3 Prohibition on Copying Office Installed Software: Under no circumstances shall individual staff members copy office-owned software for installation on personal or any other IT resources.

516.14 Private Sensitive and Confidential Information

Private sensitive and confidential information requires specific protections. Unauthorized access or disclosure may result in reputation, regulatory, and/or financial harm to UCAT, its staff, and/or its clients. All information systems—automated and manual—used by UCAT must adhere to levels of security consistent with the sensitivity of the information contained therein. In the absence of specific direction, information shall be treated as confidential.

14.1 Private Sensitive and Confidential Information: Users shall not retain private sensitive information (516.4.4) or confidential information (516.4.5) on UCAT-owned IT resources, unless: (1) the user requires such private sensitive or confidential information to perform duties that are necessary to conduct the business of UCAT; (2) the cognizant associate or assistant commissioner grants written permission to the user; and (3) the user takes reasonable precautions to secure private sensitive information, including the use of encryption on portable or mobile IT resources. Users shall not retain UCAT private sensitive or confidential information on non-UCAT-owned IT resources.

14.1.1 Private sensitive or confidential Information shall not be left on printers, copy or fax machines, etc. for extended periods of time. Information shall not be left on white boards, flip charts, or in conference rooms. Information found in inappropriate areas should be returned to the owner, if known, or removed and securely stored until the owner is found or identified.

14.2 Encryption: Encryption methods must be employed to protect private sensitive information contained on mobile or other portable devices, and information sent over public computer networks.

14.3 Backups: Critical UCAT information which is stored on mobile IT resources shall be regularly backed up and these backups shall be protected against disclosure, theft, or loss.

14.4 Release of Information: A nondisclosure agreement shall be signed by all UCAT employees (including full- and part-time employees), contractors, interns, etc. who will

have access to private sensitive and confidential information. Legal agreements assuring the protection of private sensitive information shall be in place prior to the exchange, release, or transfer of such information to external users, including the Utah State Board of Education, the Utah System of Higher Education, the Utah Department of Workforce Services, etc.

205.15 Prohibited Activities

No UCAT IT resource shall be used in any way that violates UCAT's Information Technology Acceptable Use Policy (516), state or federal law, or generally accepted standards of computer ethics and etiquette. This includes, but is not limited to, the generation of threatening, harassing, abusive, obscene, or fraudulent messages. IT resources may not be used in a manner that involves or facilitates any of the following prohibited uses, even during limited personal use:

15.1 Any infringement or misappropriation of copyrighted material or software, trade secrets, or other intellectual property;

15.2 Any attempt to gain or help others gain unauthorized access to, or anything that jeopardizes the security of IT resources, data, or confidential information, or the privacy rights of others;

15.3 Engaging in or facilitating any crime, fraud, or illegal act, including gambling and sports pools;

15.4 Racist, sexist, stalking, harassing, or threatening communications (See Policy 502, Sexual Harassment and Consensual Relationships);

15.5 Any use that is for the personal gain of an employee or another person, including selling access to UCAT material; personal business; endorsement of products, services, or commercial enterprise; or to solicit for charitable organizations not approved and sponsored by UCAT;

15.6 Any misrepresentation of identity in accessing confidential information or in sending an electronic message, including sending a message as an official UCAT communication without appropriate permission. Users shall take steps to correct misrepresentations if they have mistakenly falsely identified themselves;

15.7 Distribution, communication, access, download, or display of pornography or material that is sexually explicit, excessively violent, harassing, or otherwise offensive;

15.8 Destruction, damage to, or alteration of any UCAT IT resource or property without proper authorization, or any unauthorized change to the design or configuration of IT resources, including the installation of non-UCAT-approved screen savers or downloading executable software that is not approved by an IT resource administrator;

15.9 Any unauthorized activity that interferes with or adversely affects the performance of the employee's work or the work or responsibilities of others using UCAT's networks and systems, such as implementing or propagating a computer virus, using destructive software, inappropriate game playing, or monopolizing information resources for entertainment or personal use;

15.10 Sending or forwarding unsolicited bulk e-mail, chain letters, or "spam";

15.11 Any attempt to circumvent or disable security, monitoring, filtering, auditing, or other UCAT systems; engage in any activity that might be harmful to systems or information stored thereon; or interfere with the operation thereof by disrupting services or damaging files. Examples include but are not limited to: running "password cracking" programs, attempting to read or change administrative or security files, attempting to or running administrative programs for which permission has not been granted, using false identification on a computer or system or using an account assigned to another, forging mail or news messages, etc. Exceptions are to be approved by the Commissioner of Technical Education and shall be reserved only for approved “penetration tests” and other information security reviews;

15.12 Any attempt to monitor or tamper with another user's electronic communications, or to copy, change, or delete another user's files or software without the explicit agreement of the owner(s); and

15.13 Campaigning or other political activities, including lobbying Congress or any government agency.

516.16 Monitoring

16.1 **Privacy and Security:** Users shall respect others’ legitimate expectations of privacy. However, the security and privacy of electronic records cannot be guaranteed. Appropriate administrators may require access to users' email and other electronic records typically taken to be private:

16.1.1 Individuals having electronic communication system administration responsibilities, who cannot perform their work without access to email and other records in the possession of others, may access such information as needed for their job responsibilities.

16.1.2 Through the course of system maintenance, IT resources administrators may view the contents of records as they are processed through the electronic communications system. However, these staff members are expected to maintain the confidentiality of any data they encounter in accordance with this policy. Not doing so may subject IT resources administrators to disciplinary action up to and including termination.

16.1.3 Electronic documents may be disclosed pursuant to public records law or in the discovery process.

16.2 Monitoring: UCAT reserves the right to monitor any or all aspects of its IT resources. UCAT may monitor IT resources as a routine matter to the extent permitted by law, when monitoring is deemed necessary to maintaining the integrity and effective operation of its IT resources. UCAT may also engage in "responsive monitoring" in response to a particular problem, complaint, investigation of a claim, or lawsuit. Such responsive monitoring will be approved by the Commissioner of Technical Education. All monitoring shall comply with the following restrictions:

16.2.1 All monitoring shall be relevant to a specific UCAT purpose, problem, complaint, investigation of a claim, or lawsuit;

16.2.2 Disclosure and use of resulting data shall be restricted to UCAT-related purposes; and

16.2.3 Monitoring a person's email must be approved in writing by the Commissioner of Technical Education.

16.2.4 Advice from legal counsel may be sought before permission to monitor is granted.

16.3 Monitoring Activities: To conduct its monitoring activities, UCAT may:

16.3.1 Record telephone calls made by or placed to staff members;

16.3.2 Generate telephone usage reports;

16.3.3 Review computer and network usage;

16.3.4 Scan, review, and record incoming/outgoing email and instant message activity;

16.3.5 Track every instance of internet connection and specific website access; and

16.3.6 Review system resource usage logs including disk space, remote access, log-in, and other system logs.

16.4 Child Pornography: As provided in UCA 76-10-1204.5, IT resource administrators who, through the course of their employment, view an image on a computer or other electronic device that is or appears to be child pornography shall immediately report the finding of the image to a state or local law enforcement agency, or to the Cyber Tip Line at the National Center for Missing and Exploited Children. The IT staff shall also report the finding to the Commissioner of Technical Education. An IT resource administrator who willfully does not report such an image is subject to punitive action(s) described in Utah Criminal Code.

Subject:	Information Technology Acceptable Use

516.17 Incident Reporting and Disciplinary Action

17.1 Security Incident Reporting: All suspected or actual security breaches of UCAT IT resources shall immediately be reported to an IT resource administrator. IT Resource Administrators shall report security incidents to the Commissioner of Technical Education.

17.1.1 If private sensitive information has been accessed or compromised by unauthorized persons or organizations, the IT resource administrator responsible for the information shall consult with the Commissioner of Technical Education and any applicable external resources necessary (e.g., Division of Risk Management, Attorney General's Office, etc.) to assess the level of threat and/or liability posed to UCAT and to those whose private sensitive information was accessed. Based on an assessment of the risk, UCAT may decide to notify individuals whose private sensitive information was accessed or compromised and provide information regarding measures to be taken to protect themselves from identity theft.

17.1.2 Mobile IT resources must be sanitized if lost or stolen when applicable technology and functionality exists.

17.1.3 If a virus is suspected, users shall notify an IT resource administrator immediately.

17.2 Report Non-compliance: Incidents of actual or suspected non-compliance with this policy shall be immediately reported to the IT resource administrator.

17.3 Suspension of Access

17.3.1 An IT resource administrator may immediately suspend a user's access to IT resources when the administrator reasonably believes:

(a) The user has violated office policies or law; and

(b) The user's continuing use of IT resources will result in: (1) damage to IT resource systems; (2) further violations of law or policy; or (3) the destruction of evidence of such a violation.

17.3.2 A user whose access to UCAT IT resources has been suspended shall be informed of his or her right to immediately appeal such a suspension to the Commissioner of Technical Education. The Commissioner shall be the final arbiter over the matter.

17.3.3 Users who are not UCAT employees may have their access to IT resources unilaterally revoked without warning if they violate this policy.

17.4 Disciplinary Action: Personal use of UCAT's IT resources is a privilege rather than a right. Staff members using the systems in an appropriate manner and on an occasional personal basis need not be concerned about monitoring activities or possible disciplinary actions. However, misuse of any of these systems or other violation of this policy may subject a staff member to disciplinary action up to and including termination of employment in accordance with Policy 525, Evaluation, Corrective Action, and Termination of Staff Personnel.

516.18 Staff Separation

18.1 Preparing for Separation: A UCAT employee, upon deciding or learning of an impending separation from the organization, shall work with an IT resource administrator to establish procedures for: (1) the archival of applicable UCAT information in the employee's possession in accordance with established record retention schedules; (2) the return of UCAT-owned IT resources in a timely and efficient manner that does not interfere with the employee's remaining operations; and (3) the deletion of UCAT materials on privately-owned IT resources.

18.2 Retained Access to Email: UCAT Employees shall retain access to their business email accounts for thirty days after separation from the organization, after which time access shall be terminated. Former employees are still expected to adhere to the Information Technology Acceptable Use policy (516) until their email access is terminated.

18.3 UCAT Access to Former Employees' Email: UCAT reserves the right to examine and indefinitely retain electronic messages contained in a former employee's email account for such time as the information is required or may prove useful to UCAT business operations. Unauthorized access to former employees' email accounts, or access thereto for non-business-related purposes, is strictly prohibited.

18.4 Deletion of Email Accounts: Former employees' email accounts, including all messages contained therein, shall be deleted when applicable records retention requirements have been satisfied and the information is no longer useful.

516.19 Final Disposition of Information Technology Resources

19.1 IT Replacement Schedules: An IT resource administrator shall work with the Assistant Commissioner for Planning, Finance, and Facilities to identify and maintain replacement schedules for all inventoried IT resources (516.12.1).

19.2 IT Resource Sanitization: IT resources that have been replaced or are otherwise no longer necessary shall be thoroughly sanitized, ensuring the complete destruction of private sensitive and confidential information.

19.3 Final Disposition: IT resources that have been replaced or are otherwise no longer necessary, and that have been thoroughly sanitized, shall be disposed of in accordance with established surplus/disposal procedures.