School of Communication and Information
Rutgers, The State University of New Jersey
4 Huntington Street
New Brunswick, NJ 08901-1071

comminfo.rutgers.edu
Phone: 848-932-7500
Fax: 732-932-6916

Policies Related to Purchases, Support, and Protection of Hardware, Software, Data, and Technology Services

Last updated April 30, 2019

The School of Communication and Information supports the technology needs of its faculty and staff in the performance of teaching, research, administration, and other job responsibilities. In many cases SC&I provides the infrastructure, hardware, software, and IT services that are needed by departments, programs, and individuals in the school to accomplish goals related to the mission of the school. We also assist those who have particular IT needs to help them select the appropriate technology tools, and either provide support, or advice in finding support, for technologies that they choose to adopt.

A key principle for the school's information technology function is that it should be value-added; we strive not to duplicate technology or services that the university provides. Because of the innovative research and teaching methods in use at the school, SC&I often adopts technologies in advance of the university (email about six years before the university, VoIP phone service about ten years before the university, lecture-capture several years before the university), but when the university later adopts technology with similar functionality, our practice is to participate in the university system and focus our limited efforts on services only we can provide.

The IT Services website at http://its.comminfo.rutgers.edu provides details about the technology and services offered by the school.

This policy outlines the principles and practices used by the School of Communication and Information in providing hardware, software, and services. While we attempt to support the widest range of hardware and software possible, staffing and other resource constraints mean that there are limits to our operations and support.

PURCHASE OF TECHNOLOGY

All hardware purchased with university funds must be tagged for inventory purposes. This applies to items purchased through IT Services, faculty support staff, purchase order, or expense reimbursement.

All devices, excluding phones and tablets, purchased through SC&I IT Services must be configured so that the IT office has an administrative account on it to assure the device meets compliance and security requirements at Rutgers.

Staff: The school provides from its central resources a computer, two monitors, and a desktop printer to each full-time staff member. In general there are standard models and set-ups available, with small individual preferences allowed. When there is a business case for a staff member to be assigned a laptop computer, such as when the position must routinely work from locations outside SC&I, the school will provide the laptop. Computers, monitors, and printers for part-time staff are addressed on a case by case basis. Any optional equipment a staff member needs or wants such as headphones, speakers, tablets, cameras, or webcams, comes from the departmental budget and therefore must be discussed with the supervisor. Those equipment purchases must be made with the consultation of IT Services as well.

Full-time faculty: Faculty members are provided with start-up and annual support funds so they can purchase the desktop and laptop computers, printers, and accessories they need for their work. Faculty may have other university support funds with which to purchase equipment as well, such as funds from teaching a Byrne Seminar, and may also have external funding that allows such purchases. Faculty discuss their technology needs with IT Services, who then obtain quotes for all non-consumable equipment. Upon faculty approval of a quote, ITS coordinates with the Business Office to have the order processed and charged to the appropriate faculty financial accounts. As with staff equipment, ITS receives the items, reviews them, adds them to an inventory list, affixes asset tags, and configures, secures, and sets up the equipment.

It is not possible for IT Services to support every brand and model of every computer, monitor, or printer. Faculty who choose to purchase unique hardware may be asked to acknowledge in writing at the time of purchase that there may not be support from IT Services for that hardware.

It is understood that sometimes equipment purchased with university funds may be used by a faculty member at home. If the purchase was made through IT Services, the helpdesk will provide support for that equipment, but it may need to be brought into SC&I in order to be serviced. All such devices and software are expected to be maintained in compliance with system and security standards of the school. Note that supplies for such equipment – such as ink cartridges for home printers – are charged to a faculty member's support funds rather than the school's IT Services budget.

Faculty who need non-computer equipment such as cameras to teach a class should work with their chair, the program director, and the program faculty to agree on adoption of such equipment appropriate for everyone who teaches that particular course. The school is in the process of determining staffing and best practices for support of audio-visual equipment given the curricular expansion requiring such material.

Centers, labs, work groups: Faculty who work in designated centers or labs, or who work in research groups with students formally or informally, generally use their support funds or external funds to procure any equipment needed for those students. As with other purchases, IT Services should be involved when hardware and software is being ordered to assure the items meet system and security standards, can be supported through normal use, and are processed through IT Services upon arrival.

When a faculty member is submitting a grant that will require significant hardware or software, IT should participate in the work plan to assure the project can be supported successfully. When an externally funded project makes use of information technology and services such as web design, website hosting, application development, or system administration beyond what the school generally provides, or has significant needs for resources such as bulk printing, the school will work with the group to consider the most appropriate work plan and financial model. The school will work with the Office of Advanced Research Computing when that is possible and appropriate. IT Services continually assesses the needs of the school and makes recommendations to the Dean's Office about new staff, technology, and services that the school should be providing to meet faculty and research team needs.

Part-time faculty and doctoral students: Part-time faculty and doctoral students share several common spaces around SC&I buildings, and the school provides a small number of computers, monitors, and printers to be shared in those spaces. The computers are typically the same as those in the school's computer labs:

they do not allow data to be saved to the hard drive in order to prevent viruses and misuse, and they are set up to assure connectivity to the wired network and to printers.

If a part-time faculty member is teaching a class that requires specialized software, and the department has agreed to the adoption of that software, the school will provide a copy/license of that software to the individual.

Personal devices: SC&I cannot be responsible for servicing personal devices, defined as devices purchased with non-university funds. Any faculty or staff member who brings their personal equipment to use at SC&I may not be able to access the SC&I network and/or school services. Through use of a NetID, the device may be able to get on RU Wireless and access services available on the web, but it may not be able to print to school printers or access other services. The school will not provide wired access to a personal device on our network, and we cannot install certain software packages available through the university that have exclusions of non-Rutgers devices. Personal computers will not be able to join the SC&I domain or access shared drives; to access shared drives those devices would have to VPN into a SC&I computer, if allowed.

A particular issue related to personal computers is their use for instruction in classrooms. Individuals who expect to connect a personal device to a classroom podium will need to provide their own adapter to connect. The large number of adapters in the marketplace (the many different types, and generations of each type) means that than the school cannot keep all of them on hand; even when some adapters were kept by the helpdesk, they were so often not returned that it is not possible for the school to provide this service.

The university makes some software available for download to personal devices as well as university devices, and all employees are encouraged to make use of this resource.

Classroom technology: In cooperation with Digital Classroom Services, SC&I supports the dedicated equipment in each school classroom. Support of classroom technology is by university policy the highest priority; anyone teaching in a classroom can and should expect working equipment in that room and should call IT Services immediately if there is a problem. However, as outlined above, IT Services cannot support personal computers that are connected to classroom podiums. Instructors should plan to use a flash drive, upload material to the web or cloud service, or make other arrangements to use the podium computer when teaching a class.

The podiums in general purpose classrooms are by policy not modified, since they are supposed to remain all the same. Podiums in SC&I-controlled classrooms, especially computer labs, may have additional software made available when needed for instruction. IT Services puts out a call in advance of each term for such requested upgrades and must coordinate sometimes conflicting requests as well as possible.

For all information technology at SC&I: IT Services must maintain physical and electronic access to all equipment, even equipment being used by research groups, to assure compliance with security requirements and Rutgers' acceptable use policy.

If a device is purchased through personal funds and submitted for expense management, the university will not reimburse for insurance or extended warranty for that device. If a device is purchased through a university purchase order, the university can cover optional warranty for extended battery protection and

accidental damage. The school requires such optional coverage for a laptop, tablet, or other device that is mobile.

PURCHASE AND USE OF MOBILE DEVICES AND MOBILE DEVICE DATA PLANS

There may be cases when a faculty or staff member can make a business case for having a Rutgers-owned mobile phone and data plan to support his/her work. Typically such an individual would have responsibilities that involve extensive off-hours and/or off-campus work. If the case is approved, a faculty member would be using support funds and a staff member would be using departmental funds for the purchase.

In these cases, a phone and data plan will be obtained through the university purchasing system and 100% of the device and service plan would be covered through the purchase order. The device and phone number then belong to Rutgers but are assigned to the individual for their use; the device has university-required security on it, and remains with SC&I should the individual leave the university. SC&I IT Services does not provide support for the cell phone hardware.

Faculty members who wish to use their support funds to purchase a pad or tablet device may arrange such a purchase through the IT Services staff using a purchase order. As with laptops, the annual support may cover the full cost of the device. Faculty who also wish to purchase a data plan may present a business case to have that included on the purchase order. Staff members may be approved for a device to be purchased by their departments, as appropriate for their job responsibilities.

Faculty members who travel internationally for work can be reimbursed from their school support funds for international data plans on either school-owned or personal phones that allow them to maintain their regular level of work-related connectivity while traveling.
An employee who would like to use an email app on a mobile device to access Rutgers email must comply with the university's Mobile Device Management Policy. (See https://oit.rutgers.edu/connect/using/mdm-policy) It is possible to access email through a web browser as well.

(The school's previous IT policy offered an additional possibility which is now no longer being allowed. The previous policy allowed faculty members who used their personal cell phone for Rutgers business to use their annual support funds towards the purchase of a personal cell phone and submit for partial reimbursement of the device itself but not the voice/data plan. Up to 80% of the cost of the device could be reimbursed from the faculty member's support funds, up to a maximum of $500 (in keeping with university expense reimbursement policy). Senior staff members who regularly worked outside of the school's usual office hours or off-campus could also request reimbursement for up to 80% of a personal mobile device. This is no longer being allowed in accordance with practices across the university. The technology landscape has changed since the last policy was implemented. A similar evolution occurred when Internet access first became available. Initially the university would cover an Internet access plan for a faculty member's home, but no longer does so.)

SUPPORT FOR AGING HARDWARE

As communication and information technology ages, it requires increasing amounts of helpdesk support. At a certain point, an individual's desire to maintain an old piece of equipment conflicts with the amount of time IT staff can provide to that individual.

If a device or its operating system are no longer being supported by the vendor that manufactured it, it means the vendor is no longer providing security patches for that item and the device becomes a security risk to the school. The school will remove such devices from all university networks, and will notify the individual that the school can no longer support the device.

If a device is still being supported by the manufacturer but is beyond its expected useful age or has had extensive wear, over time it becomes very challenging to support. In these cases, the school reserves the right to notify a faculty or staff member that the device can no longer be supported.

IT staff work with individuals to help determine if the standard warranty period for a device is appropriate or a longer period should be added at the time of purchase. In general the warranty periods and useful lifetimes of devices are:

- Desktop computers: a standard warranty may be three to four years, useful life is about four to five years
- Laptop computers: standard warranty may be three to four years, useful life varies wildly based on use and care, but average may be about four years
- Tablet computers: standard warranty may be up to 90 days, useful life can be five years depending on use and care
- Cell phones: standard warranty may be up to two years, useful life may be three or four years, but note that IT Services does not support the cell phone hardware

PURCHASE AND LICENSING OF SOFTWARE AND TECHNOLOGY SERVICES

Rutgers University makes available a wide variety of software and technology services that serve the teaching, research, and administrative needs of employees. In addition, the university negotiates for discounts for other software and services that SC&I benefits from. The school uses centralized funds to procure software and technology services for faculty and staff when the software and services are critical to deliver the overall administrative services and teaching/educational mission of the school. The provision of such items is generally by purchasing copies of software or licensing with a vendor for the number of users required.

Academic programs and the teaching mission: The school asks each academic program to determine the software and services required for teaching its classes. Individual faculty decisions about the needs for particular classes should be approved by the program faculty as a whole to assure that the school is not asked to purchase different software for different sections of one class being taught by several people. When a part-time lecturer or PhD student is teaching a class, we will provide them with a copy of the approved software and, when appropriate, install copies of it on all computer lab machines. Students will have to purchase or license the software as they would a textbook.

IT Services and Instructional Design and Technology Services should be included in the discussion about technology to be adopted by programs. They are aware of academic and Rutgers-negotiated discounts available for particular products which may affect the decision making. They also need to understand what levels of support are required by students in those classes. If a technology is adopted for a class that IT Services is not able to support, they can work with the department to outline alternatives.

The school will also centrally procure software and services that underpin the research needs of a critical mass of faculty. In some cases such as Nvivo and Qualtrics, we pay into a university pool and everyone is entitled to access them. When faculty need other software and technology services for their particular research needs, they should discuss with IT Services to see if there is a university license that they or the school can access. When the school does not provide the software or license, the faculty member should use the support funds provided to them by the school and make the purchase through university procurement whenever possible. IT Services will work with the faculty member to either provide support or identify alternate means of supporting the software use.

Rutgers University has contracts and discounts available for a wide variety of software and services that help offset costs for many purchases. To access these contracts and discounts, items must be purchased through the university and not through expense reimbursement.

If faculty or staff purchase software that is not supported by IT Services, the approver of the purchase order or expense reimbursement will ask that individual sign an acknowledgement that the school does not provide support for that item.

[Future development of this policy should address student use of software.]

Software Request Guidelines for Faculty and Instructors

- Read SC&I's "Policies Related to Purchases, Support, and Protection of Hardware, Software, Data, and Technology Services"
- Review the technology services available to SC&I instructors and their students at http://go.rutgers.edu/1y3wc2hh
- Discuss software teaching needs with your department chair, program director, and colleagues
- All software requests must be approved by the department/program before being submitted
- Validate that funds are available for the purchase

Please consult with IT Services and IDTS in formulating your requests. All requests are subject to their approval.

Online Request Form: To request that the school installs software, complete the form at: https://goo.gl/forms/mW5mkyZBlKYuTjJb2 which asks for the following information:

- Course Title
- Course Number
- Name of instructor(s)

- The approximate number of students who will be using the software, including your class and any other classes that would potentially access it.
- Is this class approved as part of the campus core requirement? ___yes ___no
- List the number of legal copies (standalone, site license) needed.
- Provide the name of the software application with vendor and pricing information (including upgrade info).
- For which computer lab is this software intended? (CI-114A, CI-114B, CI-119, CI-222)
- How often will the software be used? (e.g., once a week for 20 person class for two semesters, or used by all courses scheduled in CI-119 at least once a week)
- Are there any special hardware, disk space, or network requirements needed to support the software?
- Is the software available in other labs on campus? See the following for lab software at Rutgers: http://go.rutgers.edu/6zc5pjk2
- Is an academic and/or student version of the software available?

Deadlines for Requests

- For use in the fall term: request by June 1
- For use in the spring term = request by October 1
- For use in the summer term = request by March 1

Requests submitted after the deadline may not be available for the start of the specified term.

Request Review Process

- Requests related to upgrades of existing applications as well as new software should be submitted via the application process described above.
- Priority will be given to requests that benefit the greatest number of students in coursework and for which there do not exist good substitutes already on campus.
- A subcommittee of IDTS and ITS will review requests and analyze based on
    - Total cost
    - Legality – whether the software can be used in a lab setting
    - Technical feasibility – whether the software is compatible with the school's hardware and other installed software
    - Logistics – whether there are course scheduling issues or other issues related to the installation

Notification

- Departments and faculty will be notified via email when the software is being obtained or if there is a problem with implementing it.
- If IT Services and IDTS determine there are problems implementing the software, a meeting will be scheduled to discuss with the chair and faculty member to find a solution to the technology need.

Instructor Responsibility

- The instructor should plan to test the software after it is installed in the labs before the start of classes.
- IT Services and IDTS cannot provide training or support for special software. We strongly advise instructors to provide their own training for the software to their students and/or utilize resources such as Lynda.com for this purpose.
- Instructors who need assistance in creating software training materials for students should contact IDTS (sci-idts@comminfo.rutgers.edu).

TECHNOLOGY REPLACEMENTS AND UPGRADES

Inventory is kept of all devices purchased with university funds, whether purchased through a purchase order or expense reimbursement.

When a replacement device is purchased, faculty and staff will be asked to return the old device to IT Services unless the old device will be in continued use. In cases of software and licenses for which someone is entitled to just one instance, the software or license will be migrated from the old to the new device. However, some cloud-based software purchases/licenses allow for use by multiple devices by a single user which may make it possible to retain the old device and have it retain its full use. Both devices are still owned by Rutgers and must be returned when no longer in use.

If someone loses or damages a university-owned device as a result of their own inadequate measures to prevent theft or damage, the school will not pay to replace the device.

DISPOSITION OF TECHNOLOGY WHEN SEPARATING FROM THE UNIVERSITY

All equipment and software purchased with Rutgers funding is the property of Rutgers University. An employee in possession of any electronic device, software copy, or license for software or service made with Rutgers funds - whether through a purchase order or expense reimbursement – who leaves Rutgers will generally be given the opportunity to either purchase the item from the university at resale value or return the item to the school. Any software that was made available to the employee on a device he/she purchases from the school will be removed before the resale to the employee unless arrangements for purchase of that software or license are explicitly made and as long as the software is permitted on equipment not owned by the university.

LOANER EQUIPMENT

The school maintains some equipment which can be loaned out to a faculty or staff member when their regular devices are being serviced and in case of other short-term urgent needs.

Registered student organizations may borrow equipment for hosting hybrid meetings, request posters for hosted events, ask for lecture capture or videotaping of events. Working with the Office of Student Services, IT Services will provide an orientation to any student organization to explain services and support generally available, will provide loaner equipment if the group requests items that are available, and will provide other support on a case-by-case basis as possible.

SENSITIVE DATA

Research Data

Researchers who collect sensitive data from or about human subjects must abide by the terms outlined in their IRB-approved research protocol. IT Services will work with researchers to assure that their electronic data is secured as required.

Protected Health Information

SC&I staff are not trained or positioned to appropriately handle Protected Health Information (PHI) data even if the requestor is comfortable with asking for help from IT Services, and will therefore avoid handling files that include such data.

Non-Public Personal Information

SC&I cooperates with the university in assuring security for personal data and Non-Public Personal Information (NPPI) held on any university device or database. Our policy and strategies outlined below either duplicate or augment university policies regarding such information.

Important Definitions

Non-Public Personal Information (NPPI): As outlined by Rutgers University Policy 70.1.2, NPPI includes but is not limited to:

- Social Security numbers
- Driver's license numbers or state identification card numbers
- Credit or debit card numbers
- Medical records
- Student records
- Financial records
- Legal Records
- Police Records
- Studies or surveys using confidential or personally identifiable date
- Birth Date

University departments should not collect or use a Social Security Number, with the exception of temporary use to process a new employee. Employees can be identified through their Employee ID number from the university's HCM personnel system, and students can be identified through use of the RU ID.

Classification of Data: Classifications are helpful in determining the level of risk involved related to various forms of data. Rutgers uses three classifications.

Restricted Data (highest level of sensitive): Restricted Data is the most sensitive information and requires the highest level of protection. This information is usually described as "non-public personal information (NPPI)" and is related to people or critical business, academic, or research operations under the purview of the Owner/Data Custodian. Restricted data includes, but is not limited to, data that Rutgers is required to protect under regulatory or legal requirements. Unauthorized disclosure or inappropriate use of restricted information could result in adverse legal, financial, or reputational impact on the university. Examples of Restricted Data include but are not limited to: sensitive student or employee identifiable information (i.e., Social Security Number, driver's license number, etc.), credit card information, confidential research, and file encryption keys, as well as certain financial records, medical records, legal records, student records, police records.

Limited Access Data: Limited Access Data is information that does not meet the requirements of restricted data but requires a moderate level of sensitivity and protection from risk and disclosure. Limited Access Data is the default and should be used for data intended for use within the university or any of its units with a legitimate need-to-know. Limited Access Data may be information one unit decides to share with another outside their administrative control for the purpose of collaboration. Unauthorized disclosure or inappropriate use of Limited Access Data could adversely impact the university, individuals, or affiliates but would not necessarily violate existing laws or regulations. Examples of Limited Access Data include but are not limited to: incomplete or unpublished research, internal memos or reports, personal cell phone numbers, project data, data covered by non-disclosure agreements. Although most Limited Access data is not technically NPPI, in many cases, we will agree to protect it in the same manner in order to comply with the security requirements of organizations providing data as part of grant requests. In addition, if there is any concern that limited access data should be better protected, please contact the Information Technology Services group for assistance or guidance.

Public Data (low level of sensitivity): Public Data is information that may or must be open to the general public. It is information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to university disclosure rules, is available to all individuals and entities both internal and external to the University. While the requirements for protection of public data are less than that of Restricted and Limited Access Data, sufficient controls must be maintained to protect data integrity and unauthorized modification or destruction. Examples of Public Data include but are not limited to: data on websites intended for the general public, course listings, press releases, marketing brochures, university maps, and annual reports. Typically, we do not protect any public data with NPPI restrictions or protections, nor are individuals required to register as a data custodian for the use of public data. If public data has been used to create new information that has value, then that information should be protected by centrally storing it on our systems within SC&I.

Data Custodian: A data custodian is anyone who has access to, stores, transmits, or uses NPPI at SC&I. This includes restricted data and limited access data that is being protected as restricted data for the purposes of grant requests or in order to provide better protection on that data.

Protecting Restricted and Limited Access Data

Everyone responsible for creating, storing, or transmitting sensitive information is required to do so in a manner which protects NPPI. Any breach of security or compromise of systems containing NPPI must be reported immediately to the Office of Information Protection and Security (IPS) (rusecure.rutgers.edu) and the SC&I Dean's Office.

Hardcopy records of personal information (e.g. paper payroll documents, DVD's or tape backups with personal information) should be kept in locked cabinets, behind locked doors. Protected hard copy data should be shredded as part of the disposal process. If there is a need to send these records to another department or external agency, the documents should be sent in a sealed envelope or other packaging, marked confidential, and addressed to a specific recipient. NPPI should never be sent via email unless encrypted.

Anyone maintaining personal information in electronic form must strictly control access by encrypting the information. Where the information is limited access and protected through passwords rather than encryption, passwords should be complex and never shared. Due to the vulnerability of information on portable/mobile devices such as laptops, external hard drives, or USB memory sticks, restricted and limited access information on these devices should be encrypted.

Cell phones and tablets with sensitive information should utilize additional security measures such as strong access codes, disabling location services, time-out screen locking, and account lockout and/or remote wiping. University data housed on portable devices (laptops, cell phones, tablets, pen drives, etc.) or transmitted to and/or stored on "cloud services" should be encrypted with the encryption key separate from the device.

Travel with electronic devices requires special precautions. Remote devices and the information they contain should be protected while accessing the Internet or not physically under the owner's control.

Because of the risks when using cloud or third party providers, anyone using such services must discuss their storage of sensitive information with the Assistant Dean for Information Technology before storing such information with a third party.

The Information Technology Services office in conjunction with the SC&I Dean's Office is responsible for managing and acting as the data custodian for these different data types in the school. Appropriately safeguarding and managing this data is a primary function of the ITS office. As primary data custodians for the school, the ITS office will identify, classify, and protect NPPI and the systems the data resides on. The ITS office will periodically scan all systems for NPPI, identify those systems with it, perform risk assessments, ensure compliance, and train users on security best practices.

Members of the School of Communication and Information community are required to know what constitutes NPPI. In addition, if an individual meets the criteria for being deemed a data custodian, that individual should:

- Register as a data custodian with the School of Communication and Information. All registered data custodians will be included in a database for tracking sensitive information usage at SC&I. Anyone who meets the criteria of a data custodian whether an employee, student, or affiliate member must register immediately upon becoming a data custodian.
- Maintain NPPI in a dedicated, centralized, and secured location.
    - Electronic information should only reside on dedicated file servers (networked drives) within the SC&I environment.
    - Hard copy information should be stored in locked drawers or filing cabinets when it is not being used. When such sensitive information is being used, the material should not be left unattended, nor should any such information be left in a room that is unlocked. The information should not be left outside of its primary storage location overnight.
- Not store electronic NPPI on local systems, portable systems, portable devices, or systems being used for remote access to the SC&I networks.
- Not store or transfer NPPI using university or personal email accounts.
- Not transport hard copy NPPI outside the confines of the school or center in which it is being held.
- Not publish NPPI to web sites or any internal or external file sharing systems other than the dedicated SC&I file sharing servers. This includes files sharing systems like drop box and replication systems like iCloud or Dropbox.
- Not take any NPPI with them should they no longer be employed by, or no longer be associated with SC&I.
- Appropriately discard unused/unnecessary NPPI as soon as possible by complying with the procedures outlined below under "Secure Removal and Disposal of NPPI."
- Notify Information Technology Services immediately if there are any possible threats related to the compromise of NPPI. This includes any security threats to computer systems using NPPI. For hardcopy information, this includes any possible breach of physical security to the locations where NPPI stored.
- Not remotely access NPPI on the secure servers at the SC&I through a VPN connection if they have any suspicion that the machine being used to connect to the information is infected with malware, spyware, or a computer virus.

Should it become necessary to store NPPI outside the parameters set forth in this policy, an exception request must be completed by the appropriate data custodian and, where necessary, be approved by the Dean's Office prior to the data leaving the School as listed below. This provision allows the Dean's office to provide the requestor with advice on best practices for ensuring additional security measures are taken to protect the sensitive information.

User Responsibilities

Data custodians are responsible for storing all sensitive information on the designated systems within the technical environment of the School of Communication and Information. The protection of these systems and the associated internal networks are the responsibility of the Information Technology Services staff. If an individual is using sensitive information based on an exception request, then that individual is responsible

for the safety and security of that data. Data custodians are expected to notify IT Services (for electronic information) or the Business Office (for hard copy information) immediately if any threats arise that may jeopardize the security of NPPI. It is also expected that any individuals acting under an exception request will adhere to any additional security related procedures recommended by the technical and business staff of School of Communication and Information Dean's office.
Should an individual associated with the school but not employed at the school become responsible for NPPI, he or she must register as a data custodian. The responsibility of notice in this regard will fall upon the area director or the principal investigator for grant related research. For centers this will be either the faculty director or the staff executive director.

Proactive Restricted Data Discovery Processes

IT Services will use scanning tools to proactively try to identify Restricted Data that resides on systems within the school to ensure that it is adequately protected. These scanning tools will be used on a regular basis and any restricted data that is discovered will result in communications with the owner of the data to ensure that the data should be stored in its current location, that it is adequately protected, and to ensure that the individual is properly registered as a data custodian. Similarly, the Business Office will periodically conduct in-person audits for hardcopy restricted data.

Secure Removal and Disposal of NPPI

Any system that houses NPPI requires special attention prior to its disposal. Specifically, NPPI will need to be securely removed so that there are no traces of that data left on the existing system or device. When such a device needs to be disposed of, IT Services should be contacted to provide assistance with securely deleting such information through drive sanitization processes. This includes computers, copiers, fax machines, and portable storage devices.

Sensitive information in hardcopy form should be destroyed once it is no longer deemed necessary by school-wide and university-wide records retention policies. Hardcopy sensitive information should be cross shredded prior to disposal. Unnecessary NPPI should remain in a locked filing cabinet or desk until it is shredded. In addition, any credit card information recorded for the purposes of processing a transaction should be destroyed immediately after completing the transaction.

Security Training

All members of the School of Communication and Information are encouraged to complete an online information security awareness training session and take a quiz associated with that training. These training guidelines are also applicable to any registered data custodian whether he or she is part of the school or not.