

80.90.007 INFORMATION ESECURITY POLICY

Information eSecurity Policy

PURPOSE

To document the desired behaviors and practices regarding the acceptable use of the Hospital's and the Graduate School's information systems.

SCOPE

The policy and its accompanying procedures apply to all Graduate School students, faculty, and staff.

STAKEHOLDERS AFFECTED BY THIS POLICY

Stakeholders affected by this policy include all Graduate School students, faculty, and staff.

POLICY

In following the acceptable use agreement, you agree to:

1.1 General Use

1.1.1 Exercise good judgment regarding the protection and security of the Hospital and the Graduate School information assets. Failure to follow security policies and standards could place the Hospital and the Graduate School in violation of laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Protection of Student Data.

1.1.2 Exercise good judgment when communicating as a member of the Graduate School over email, social media or other technology. Members of the Graduate School should not use language that may be offensive, obscene, sexually explicit, threatening, intimidating, discriminatory, retaliatory, or harassing.

1.1.3 Promptly report the theft, loss, or unauthorized disclosure of the Graduate School Confidential or Protected information (e.g., grades, student information, proprietary information) to the Graduate School and Information Security Office at information.security@stjude.org.

1.1.4 Use of Hospital or Graduate School technologies (network, Internet, email, computers, files shares and applications) is done so with the understanding that they are monitored for security purposes and there is no right

80.90.007 *INFORMATION ESECURITY POLICY*

to or expectation of privacy when using Hospital or Graduate School owned technology. The Hospital or the Graduate School reserves the right to access, monitor and disclose contents of the Internet, email, and voice mail messages or other communications made through the Hospital or Graduate School owned systems.

1.1.5 Use of Hospital or Graduate School information systems with the understanding that occasional personal use is allowed provided it is not associated with a personal business, does not interfere with productivity, and does not preempt legitimate Hospital or Graduate School business activity.

1.1.6 Refrain from attempting to test, circumvent, or defeat any security system or monitoring capability.

1.1.7 Refrain from using Hospital or the Graduate School information systems to engage in any unlawful or obscene activities that could put Hospital and/or the Graduate School at risk. Examples include, but are not limited to, the following:

- Gaining unauthorized access to any information system or network.
- Damaging, altering, or disrupting the operations of any information system or network.
- Making any inappropriate or discriminatory statements based on race, religion, national origin, sex, sexual orientation, transgender status, gender identity or expression, disability or veteran status.
- Accessing, reading, copying, storing or forwarding inappropriate or sexually explicit messages or materials.
- Engaging in illegal, fraudulent, or malicious conduct.

1.2 Asset Usage

1.2.1 Physically secure all Hospital and the Graduate School assets taken off-site at all times. Mobile devices should not be left in unattended bags, luggage, or vehicles.

1.2.2 Return all Hospital and the Graduate School issued assets upon termination of enrollment, employment, contract, or agreement. Access to Hospital and Graduate School systems, networks, and facilities will be disabled upon termination.

1.2.3 Use personal devices to store or access Hospital and Graduate School information only when authorized to do so and in accordance with defined policies and standards for personal devices.

1.3 Clear Desk/Clear Screen

80.90.007 *INFORMATION ESECURITY POLICY*

1.3.1 Log off from applications or network services when they are no longer needed and lock workstations when leaving your workspace unattended.

1.3.2 Control physical access to Confidential or Protected information at all times to prevent unauthorized access, e.g. lock doors to offices and file cabinets, do not leave Confidential or Protected documents in view, stay with visitors in areas with Confidential or Protected information, and do not leave Confidential or Protected information on and immediately remove from fax machines and printers.

1.4 Data Protection

1.4.1 Refrain from transferring or storing electronic protected health information (ePHI) or student protected data to a cloud-based service that has not been approved by Information Services and the Office of Legal Services. Using an unauthorized cloud-based service for ePHI and student data may be a violation of HIPAA and the Hospital's requirement to perform due diligence on all third-parties that process or store ePHI and the Graduate School's requirement to safeguard student records. The Graduate School has a policy and procedure to protect the security of its student records and back up all data. Individuals should refer to the policies listed as reference documents for more information on record retention and protection of student data.

1.4.2 Use only authorized technologies, applications, and/or services verified to meet Hospital and Graduate School security requirements. If an alternative application or cloud-based service must be used, you agree not to transfer or store sensitive or confidential information on such applications or services.

1.4.3 Do not forward Hospital or Graduate School business related emails containing Confidential or Protected information to a personal account.

1.5 Information System Access

1.5.1 Maintain the confidentiality of authentication credentials you have been entrusted with (e.g. passwords, PINS, badges, etc.). Your authentication credentials must not be shared.

1.5.2 Create and change your passwords in accordance with Hospital Information Services password requirements (e.g. password length, password composition).

1.5.3 Be responsible for all activities that use your credentials.

1.6 Physical Security

80.90.007 INFORMATION ESECURITY POLICY

1.6.1 Dispose of any electronic media containing confidential or protected information in accordance with Hospital and Graduate School disposal policies and standards.

1.6.2 Dispose of any paper containing Confidential or Protected Information securely using a locked disposal container or cross-cut paper shredder.

1.6.3 Refrain from using photographic, video, audio or other recording equipment, such as cameras in mobile devices, unless authorized.

1.7 Removable Media

1.7.1 Encrypt all removable media used to store Confidential or Protected information.

1.7.2 Refrain from connecting a removable media device from an unknown origin to a Hospital or Graduate School computer or information system as it may contain malware.

PROCEDURE

2.1 The Graduate School has internal procedures for addressing security breaches to protect Graduate School information (including student records).

DEFINITIONS

- **Removable media** – Portable data storage medium that can be added to or removed from a computing device or network.

REFERENCE DOCUMENTS

- Protection of Student Data Policy
- Record Retention Policy

FORMS AND OTHER DOCUMENTS

N/A

POLICY DETAILS

80.90.007 INFORMATION ESECURITY POLICY

Policy Type	Policy Revision
Policy Number	80.90.007
Policy Category	Administrative Policy
Policy Sponsor	Stacey Schultz-Cherry
Approval Authority	Dean of the Graduate School
Policy Effective Date	July 1, 2023
Policy Owner (Contact Info)	Stacey Schultz-Cherry (stacey.schultz-cherry@stjude.org)
Policy Alternate	Stacey Schultz-Cherry
Last Review Date	May 30, 2025
Next Scheduled Review Date	By June 1, 2026

REVISION HISTORY

V1.0 – May 25, 2023

V2.0 – August 19, 2024

APPROVALS

Dean of the Graduate School – Approved on May 25, 2023

Dean of the Graduate School – Approved on August 19, 2024