Guardrails & Governance: Safeguarding Institutional Data at UNC Charlotte

Tim Burns,
Chief Information Security Officer

Isabel Alele,
Associate General Counsel

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Core Issues:

- What is the information that must be protected?
- How are you expected to protect this information?
- Who is responsible for creating processes that govern data management?

Governing Rules:
Federal Laws, State Statutes
& Industry Standards
UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

Family Educational Rights and Privacy Act (FERPA)

- FERPA is a federal law that protects the privacy of student records.
- FERPA rights and obligations generally apply to “education records.” This term is defined as records that are:
  - Directly Related to the student
  - Maintained by the University
- Prior written consent is required to share education records unless an exception applies.

Exceptions

- Campus police records;
- Employment records (unless dependent on status as a student);
- Non-circulating faculty or staff records made for personal use;
- Treatment records (medical/counseling);
- Certain alumni records; and
- Information about a student learned through observation.

Permitted Disclosures of Education Records

- Directory Information;
- Written consent of the student;
- Judicial order or subpoena;
- School officials with a legitimate educational interest;
- Parents (if the student is a dependent for tax purposes); and
- Health/safety Emergency

HIPAA

- HIPAA governs the privacy and security of protected health information that is created, received, or maintained by a HIPAA covered entity or business associate (i.e., healthcare providers).

- HIPAA defines "protected health information" to exclude
  - Education records;
  - Treatment records; and
  - Healthcare information received by employers

Employee Personnel Records

- All records that are created regarding an employee's performance or the terms and conditions of their employment are considered part of that employee's personnel file.

- This includes onboarding and benefits information, payroll, annual appraisals, promotion/demotion, disciplinary information, ADA accommodations, and workers' compensation, etc.

- Personnel information can be maintained in any format, including electronic format.

Employee Personnel Records

- Most documents in an employee's personnel file are not public records; only the following items are:
  - Name
  - Age
  - Dates of employment
  - Employment contracts
  - Position/Title
  - Salary and salary increases
  - Assigned department considered
  - Date and type of dismissal, suspension, or demotion for disciplinary reasons

Employee Medical Information

- Under both federal law and North Carolina law, employers generally must keep employee medical and certain personnel information confidential.

- The specific requirements vary by statute, but the overarching principle is that medical and protected employment information should be disclosed only to those with a legitimate business need or as otherwise authorized by law.

PCI DSS

- What is PCI DSS? Payment Card Industry Data Security Standard is the set of mandatory technical and operational requirements designed to protect cardholder account data.

- At UNC Charlotte, this process is managed by E-Commerce. Reach out to E-Commerce when another party is:

  - Accepting card payments on behalf of UNC Charlotte or for goods/services to be provided to our faculty, staff, or students;

  - Integrating software to a platform that will accept card payments; or

  - Providing equipment that will accept card payments.

North Carolina Identity Theft Protection Act

- What does this statute require?
  - Strict restrictions on display and transmission of social security numbers;
  - Safe disposal of records
  - Mandatory Breach Notification
  - Consumer Empowerment Tools
  - Enforcement

Research Data

- Handling of research data must:
  - Align with the terms of the grant and any other contract;
  - Be used and safeguarded in compliance with confidentiality agreements;
  - Protect intellectual property rights; and
  - Adhere to applicable UNC System and UNC Charlotte policies

ONEIT STANDARDS & GUIDELINES

Protecting University Data

Security, compliance processes, and everyday best practices.

Data Storage & Handling Matrix

Level 0: Public
Freely Available

Authorized Services:
- Public Kiosks & Websites
- Personal & Work Devices
- Public Cloud Storage
- Email & Google Workspace

Examples:
Press releases, directory listings, published research.

Level 1: Internal
Designated Groups

Authorized Services:
- UNC Charlotte Workstations
- Network Drives (H:, J:, S:)
- Approved AI Tools & Email
- Canvas, Dropbox, OneDrive

Restrictions:
No public cloud or public AI tools.

Examples:
Budgets, internal memos, research.

Level 2: Confidential
Subject to Regulation

Authorized Services:
- Secure Network Drives
- Internal Email (Authorized)
- Approved Cloud (No Sync)

Restrictions:
Never store on personal devices. Requires encryption/access limits.

Examples:
FERPA, GLBA data, PII, Research.

Level 3: Highly Restricted
Severe Risk

Authorized Services:
- Tightly Controlled Systems
- OneIT Approval

Strictly Prohibited:
- Email & Standard Cloud
- AI Tools & Portable Media
- Workstations & Laptops

Examples:
SSNs, Medical Records, PCI Data.

For full standards & guidelines, visit https://oneit.charlotte.edu/resources/standards-guidelines/standard-for-information-classification/guideline-for-data-handling/

Handling Level 0 & Level 1 Data

Level 0: Public

Freely available information.

- Disclosure requires no authorization.
- No potential harm to the university.

- **Examples:** *Public data includes, but is not limited to: Advertising, product and service information, directory listings, published research, presentations or papers, job postings, press releases.*

Level 1: Internal

Designated groups only.

- Unauthorized disclosure would not cause adverse impact.

- **Examples:** *Internal data includes, but is not limited to: Budget and salary information, personal cell phone numbers, departmental policies and procedures, internal memos, incomplete or unpublished research.*

Handling Level 2 & Level 3 Data

Level 2: Confidential

Subject to regulations.

- Never store on personally owned devices.
- Requires encryption and limited access.

- **Examples:** *Confidential/sensitive data includes, but is not limited to: Student data that is not designated as directory information, passport data, personal financial information, certain research data (e.g., proprietary or otherwise protected), personally identifiable information (PII) such as name, birthdate, address, employee or student ID, etc. where the information is held in combination and could lead to identity theft or other misuse.*

Level 3: Highly Restricted

Severe impact if breached.

- Never export outside secured locations.
- Never email or store in cloud drives.

- **Examples:** *Highly restricted data includes, but is not limited to: Social Security Numbers, payment card numbers, medical records, restricted information protected by nondisclosure agreements, restricted research data.*

Compliance Overview for Purchases

Integration & Data Assessment

- **Integration:** Identify connected enterprise applications.
- **Level 2 Data:** Detail data types (Name, email, address, birthdate).
- **Research Data:** Confirm what data will be used or Research will be conducted.

Authentication & Access Controls

- **Non-Research Level 2:** Verify MFA or SSO availability if lacking.
- **SSO Verification**

AI & Data Usage

- **AI Training:** Confirm if customer data is used to train AI models.

Privacy Policy Review

Required for Level 2+ Data

- Secondary data usage validation.
- Security incident notification timelines.
- Post-subscription data retention & deletion policy.

Agreements & Governance

- **DPA's:** Obtain signed Data Processing Agreements.
- **Risk Acceptance Agreements**

"Need to Know" Principle

Granting minimum access required for legitimate job duties and third parties

Least Privilege

Access restricted to minimum necessary functions.

Role Alignment

Tied strictly to current university responsibilities.

No Curiosity Browsing

Never view sensitive data without a business requirement.

AI Usage Guidelines

- Only input Level 0 or Level 1 data.
- No Level 2/3 data in Public AI tools.
- Treat all AI inputs as public information.
- Assume external vendors retain your prompts.

Resources & Links:

Security Checklist: https://oneit.charlotte.edu/innovation/artificial-intelligence/security-checklist/

AI Software Guidance: https://oneit.charlotte.edu/innovation/artificial-intelligence/ai-software-guidance/

CLOUD STORAGE

Google Workspace Storage

Level 0 & Level 1

Fully permitted for storage and sharing.

Level 2 (Conditional)

Permitted only with limited access. Do NOT sync locally.

Level 3

Strictly prohibited in Google Drive.

Auditing Your Google Drive

Regularly review who has access to your files.

Check Public Links

Search Drive for files shared with "anyone with a link."

Check Domain Access

Review files shared broadly within the Charlotte domain.

Remove Inactive Users

Revoke access for graduated students or former employees.

Audit Annually

Conduct routine reviews per User Access Management guidelines.

General Data Best Practices

No Personal Devices: Never store Level 2 or Level 3 data on non-university equipment.

Use MFA: Always utilize multi-factor authentication for systems processing sensitive data.

Secure Transfers: Level 3 data must never be sent via standard email or unauthorized cloud apps.

Questions or Reporting?

We are here to help protect our university data.

General Questions: Your Unit's Information Security Liaison

Specific Compliance: ISCompliance-group@charlotte.edu

Suspicious Email: ReportSpam-group@charlotte.edu

Incidents: SecurityIncident-group@charlotte.edu

Data Governance
at UNC Charlotte
UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

Key Players in the Data Governance Process

- Executive Steering Committee
  - Role: Vision & Authority
  - Focus: Defines high-level strategy and delegates execution.
- Data Governance Committee
  - Role: Standards & Implementation
  - Focus: Establishes policies, approves data definitions, manages security levels, and handles escalation.
- Data Stewards
  - Role: Domain Ownership
  - Focus: Appointed subject-matter experts managing daily data quality, protection, and usage rules.

The Data Governance Committee

The Data Governance Committee is the collaborative body responsible for orchestrating the strategy, protection, and operational oversight of UNC Charlotte's data assets. Functionally, it establishes unified data definitions, assigns steward accountability, and creates standardized processes for requesting and accessing data. By embedding governance knowledge across all divisions, the committee ensures the use of data remain defensible while enforcing strict classification and safeguard controls.

Goals of the Data Governance Committee

- Designated Stewards
- Unified Standard Terms
- Data Integrity
- Security and Compliance
- Streamlined Data Access
- Defensible Reporting
- Shared Governance

The Pillars of Data Governance

- Authoritative Sources
- Substance > Structure
- Oversight from Creation to Disposal
- Purpose Driven Usage
- Need-Based Access
- Risk-Proportionate Controls

Questions?
UNIVERSITY OF NORTH CAROLINA
CHARLOTTE