A Place For Everything: Guidelines for Record Management and Data Handling

Division of Institutional Integrity Legal Symposium, October 26, 2023

Tina Dadio, Public Records Officer/Legal Specialist
Tarveras Rogers, IT Auditor, Certified Information Systems Auditor
Susan Wagoner, Info Security Compliance Manager

UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

Agenda

- Basic review of public records law and records retention policy
- Overview of the records retention policy
- Overview of the UNC System Retention Schedule
- Guidelines for data handling
- Levels of data classifications and types of records

First the basics – What is a public record?

- All documents of any type “regardless of physical form or characteristics…made or received in the connection with the transaction of public business by any agency of North Carolina. (NCGS 132-1(A))
- Note:
  - ➢ UNC Charlotte is considered a state agency
  - ➢ Disposition of records are governed by law: NCGS 121 (Archives & History) & 132 (Public Records Act)

What if you deny public access?

- Anyone who is denied access to a public record may seek a court action to compel the State agency to turn over the records (NCGS § 132-9(a))
- Burden is on the State (NCGS § 132-9(b))
- Presumption is that all State records are open to the public

What is Records Management?

- Methods to efficiently, effectively, and economically create, use, maintain, preserve, and dispose of official records

What is University Archives?

- Located in Atkins Library

- Collective memory of UNC Charlotte

- Collect, preserve, make available historical records

- Charged by the Chancellor to guide records management activities on campus (see University Policy 605.3)

Why do we have Records Management?

- To comply with North Carolina law
- Preserve certain history records (ongoing administrative or research value)
- Space (disposed of records that no longer have administrative value to make room for those of current and continuing value)
- Improves efficiency and costs savings (limited record storage facilities for permanent non-historical records)

Appointing a Records Manager

- Identify and appoint a Records Manager responsible for:
  - ➢ Ensuring department/unit records are retained and disposed of in accordance with Record Retention Schedule and/or unit specific schedule
  - ➢ Restricting access to confidential university records and information
  - ➢ Transferring records with historical value or permanent records to the University Archives
  - ➢ Maintaining a destruction and/or transfer log of records

Why do we have a records retention schedule?

- Identifies which records have permanent value and which ones do not
- Provides descriptions or records and when to dispose of them
- Identifies confidential or restricted records

Where do I find the retention schedule?

- UNC General Records Retention and Disposition Schedule found here
  - ➢ The North Carolina Department of Natural and Cultural Resources (NCDCR) is responsive for providing guidelines for record retention and disposition for all universities in the UNC System, as well as previous amendments to the schedule

- Also can be found here: University Policy 605.3, Retention, Disposition, and Security of University Records or on Special Collections and University Archives' site

- The Schedule describes:
  - ➢ The Series (or types) of records;
  - ➢ The length of time records must be preserved
  - ➢ How to dispose of records

Definitions

- Transitory record – records that have little or no documentary or evidential value and do not need to be set aside for the future (meeting invites, routing slips, transmittal sheets, etc.
- Reference value – a record held by an office for its own reference and not the official record for the University that hold limited value, typically documenting routine operations within the office (templates, instruction manuals, newsletters, etc.)
- Record series – a group of records that are related (personnel files, student files, contracts, business correspondence, financial statements, etc.)
- Retention period – length of time a record should be kept before disposing (ex.: transfer to university archivist after 5 years)
- Disposition – what happens to a record when it is no longer needed for current University business (3 steps: review, archive, destroy)

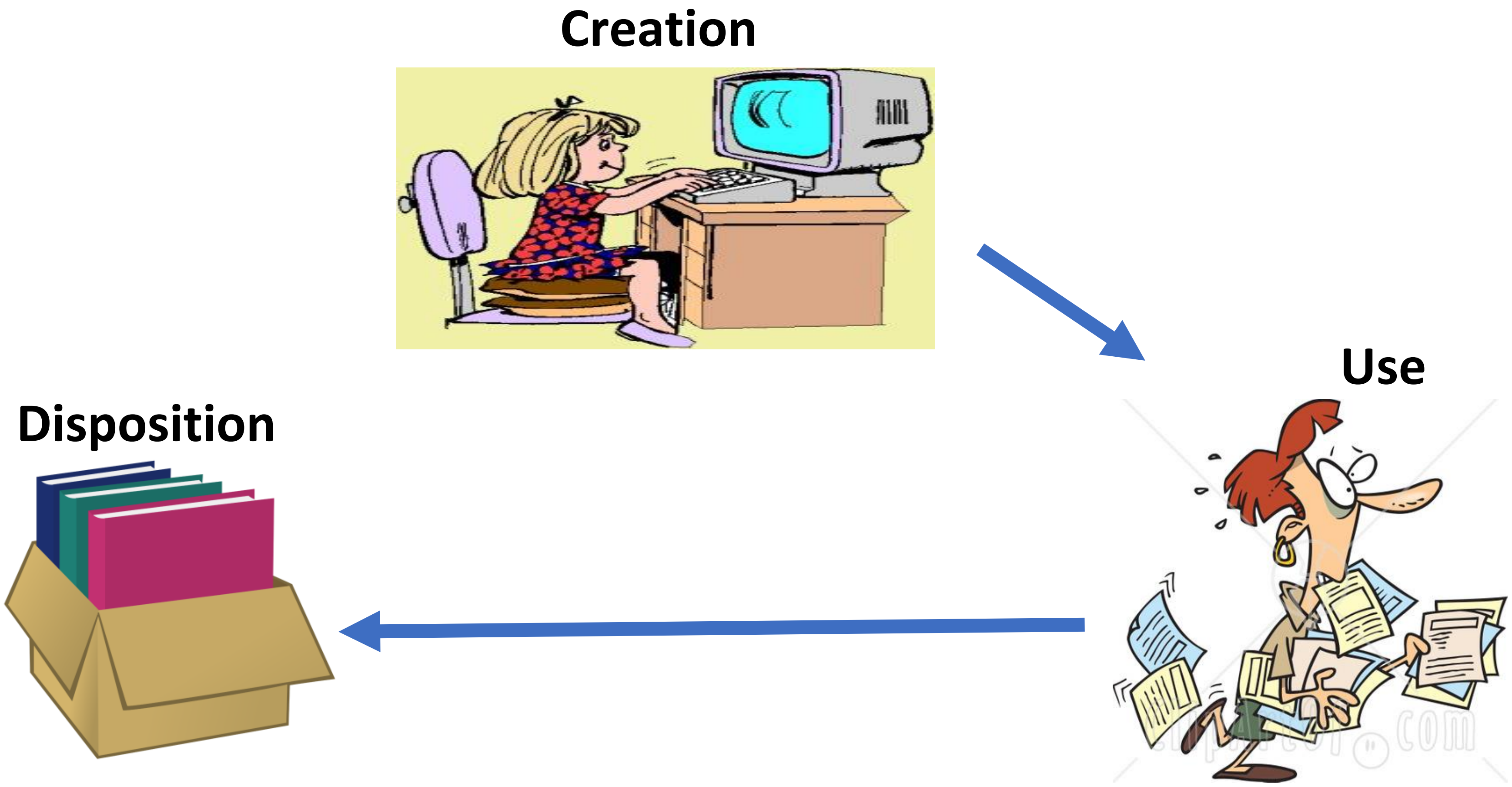
Why all the fuss?

- State law requires agencies to retain public records and prohibits the destruction EXCEPT in accordance with the guidelines established by the North Carolina Department of Cultural Resources

- Rule applies to all UNC Charlotte employees

- Remember: All UNC Charlotte employees are responsible for the records they create and maintain

Stages of a Record



Creation

Use

Disposition

Get a Handle on Electronic Records

- Assess what records your office creates
  - **Note:** It is the **<u>content</u>** not the <u>format</u> of each record that determines its retention and disposition
- Build a useful folder structure
  - Group records together by function
  - Identify records that reach the end of their retention period at the same time
  - Structure should be unambiguous with no redundancy
- Review annually
  - Communicate changes and train staff accordingly
  - Review for legal holds and archival/permanent records
  - Check-in on the plan—is it still working for your office? Modify if needed

Helpful Tips…

DO

- DO centrally locate records in shared drives (Google Drive, Dropbox, etc.)
- DO include the record series and disposition in folder titles
- DO use hierarchical folder structure
- DO label convenience copies and backups for easy deletion
- DO keep the final version
- DO use human-readable file names

DO NOT

- DO NOT store records on local hard drives or personal drives
- DO NOT make file paths too deep
- DO NOT keep each revision

What about drafts…Guidance from Schedule

"Drafts and working papers, including notes and calculations, are materials gathered or created to assist in the creation of another record. All drafts and working papers are public records subject to all provisions of N.C. Gen. Stat § 132, but many of them have minimal value after the final version of the record has been approved, and may be destroyed after final approval, if they are no longer necessary to support the analysis or conclusions of the official record. Drafts and working documents that may be destroyed after final approval include:

- ➢ Drafts and working papers for internal and external policies
- ➢ Drafts and working papers for internal administrative reports, such as daily and monthly activity reports;
- ➢ Drafts and working papers for internal, non-policy-level documents, such as informal workflows and manuals; and
- ➢ Drafts and working papers for presentations, workshops, and other explanations of agency policy that is already formally documented."

Data Classification and Handling

First the basics

- Data is one of the University’s most valuable assets.
- Employees handle sensitive and confidential data on a daily basis.
- It’s important for the University to educate employees on how to identify and properly secure data.

What should you know?

- How to categorize data into the different data classifications.
- What precautions are needed when handling different types of data.

Why does it matter?

Understanding the different levels of data leads to informed decision-making and good security practices:

- ➢ Where can the data can be stored?
- ➢ Who is authorized to view the data?
- ➢ Can the data be copied from the original location to a different location?

Data Classification Levels

4 Data Classification Levels

Level 0 -- Public

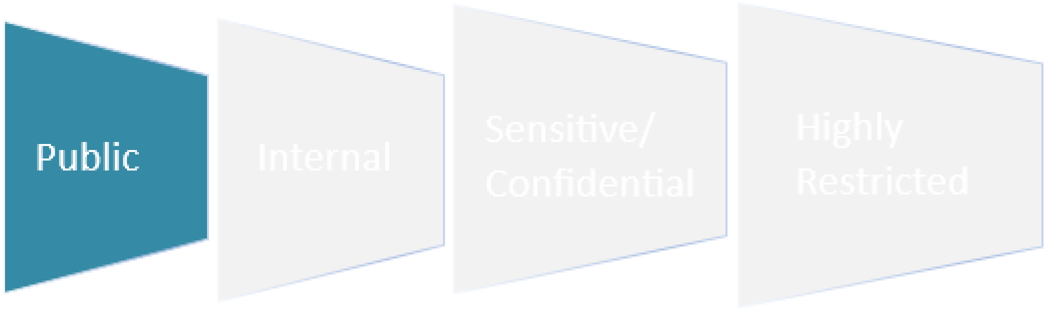
Level 1 -- Internal

Level 2 -- Sensitive/Confidential

Level 3 -- Highly Restricted

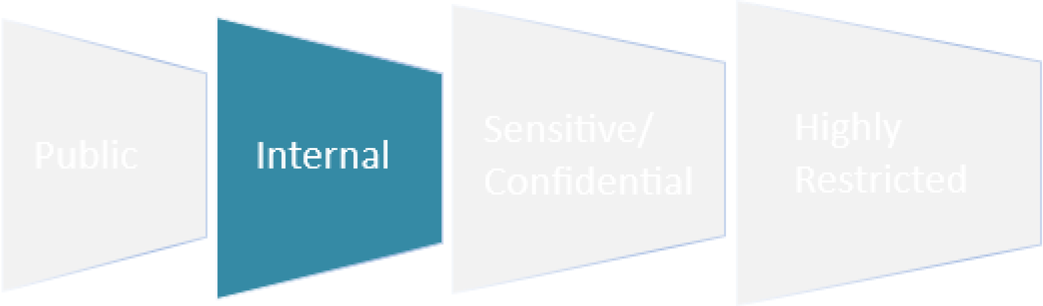
Level 0 - Public

- Can be made generally available to the public and requires no authorization to share.
- Examples: Websites, Press Releases, Directory Listings, Job Postings.
- Handling: Can be stored anywhere.



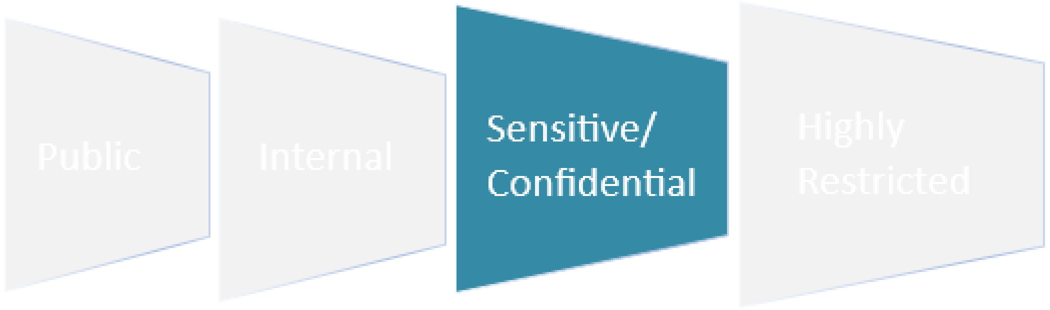
Level 1 - Internal

- Not generally shared with the public without appropriate authorization.
- Examples: Department Procedures, Internal Memos, Budget Information.
- Handling: Can be stored on University devices, network drives, Google Drive, Dropbox.



Level 2 – Sensitive/Confidential

- Data loss or unauthorized disclosure could have serious adverse impact. Often protected by statutory, regulatory, or contractual requirements.
- Examples: FERPA Data, Personnel Records, Financial Information, Personally Identifiable Information (e.g., name + address + DOB + email + phone number).
- Handling: Can be stored (with appropriate access) on network drives, Google Drive, Dropbox, can be sent internally via email. Should not be stored on local hard drives.



Public

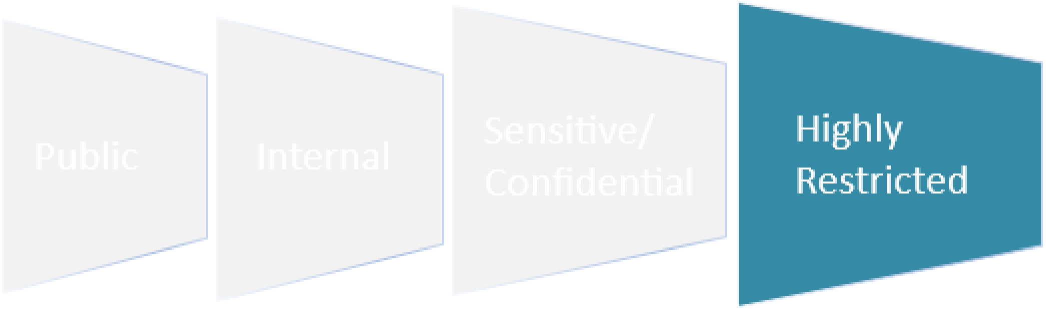
Internal

Sensitive/ Confidential

Highly Restricted

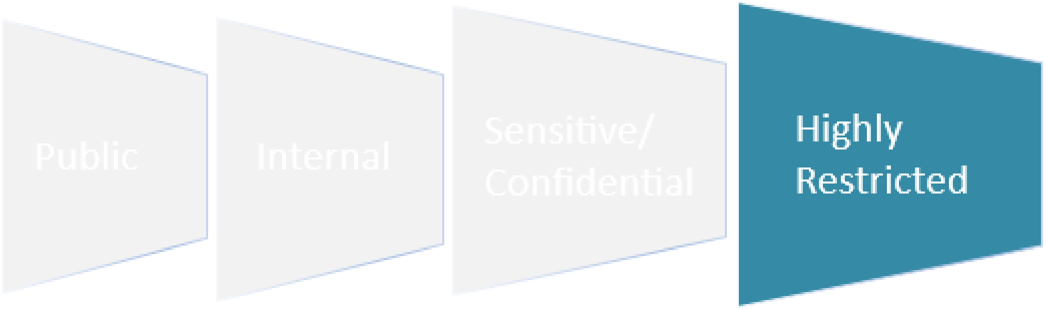
Level 3 – Highly Restricted

- Data loss or unauthorized disclosure could lead to financial loss, impair the University’s ability to conduct business, cause reputational loss, or result in a violation of laws, regulations, or contractual agreements.
- Examples:



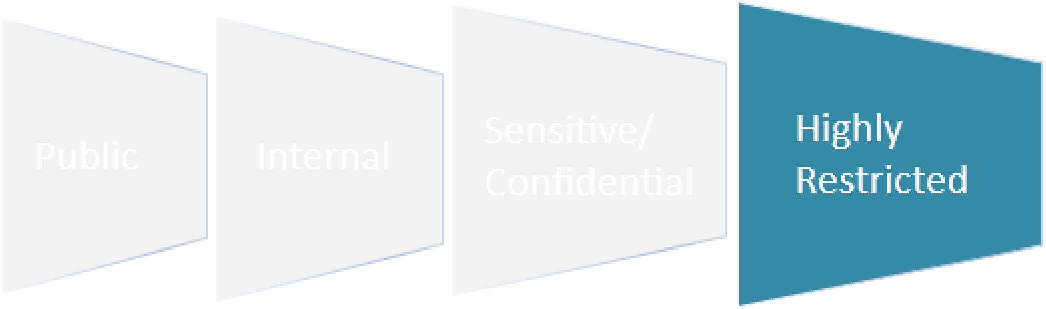
Level 3 – Highly Restricted

- Data loss or unauthorized disclosure could lead to financial loss, impair the University's ability to conduct business, cause reputational loss, or result in a violation of laws, regulations, or contractual agreements.
- Examples: SSNs, Credit Card Info, Sensitive Health Info, Data protected by Non-Disclosure Agreements.
- Handling:



Level 3 – Highly Restricted

- Data loss or unauthorized disclosure could lead to financial loss, impair the University's ability to conduct business, cause reputational loss, or result in a violation of laws, regulations, or contractual agreements.
- Examples: SSNs, Credit Card Info, Sensitive Health Info, Data protected by Non-Disclosure Agreements.
- Handling: Very tightly managed requiring explicit authorization to view. <u>Should not be exported or downloaded without express permission</u>.



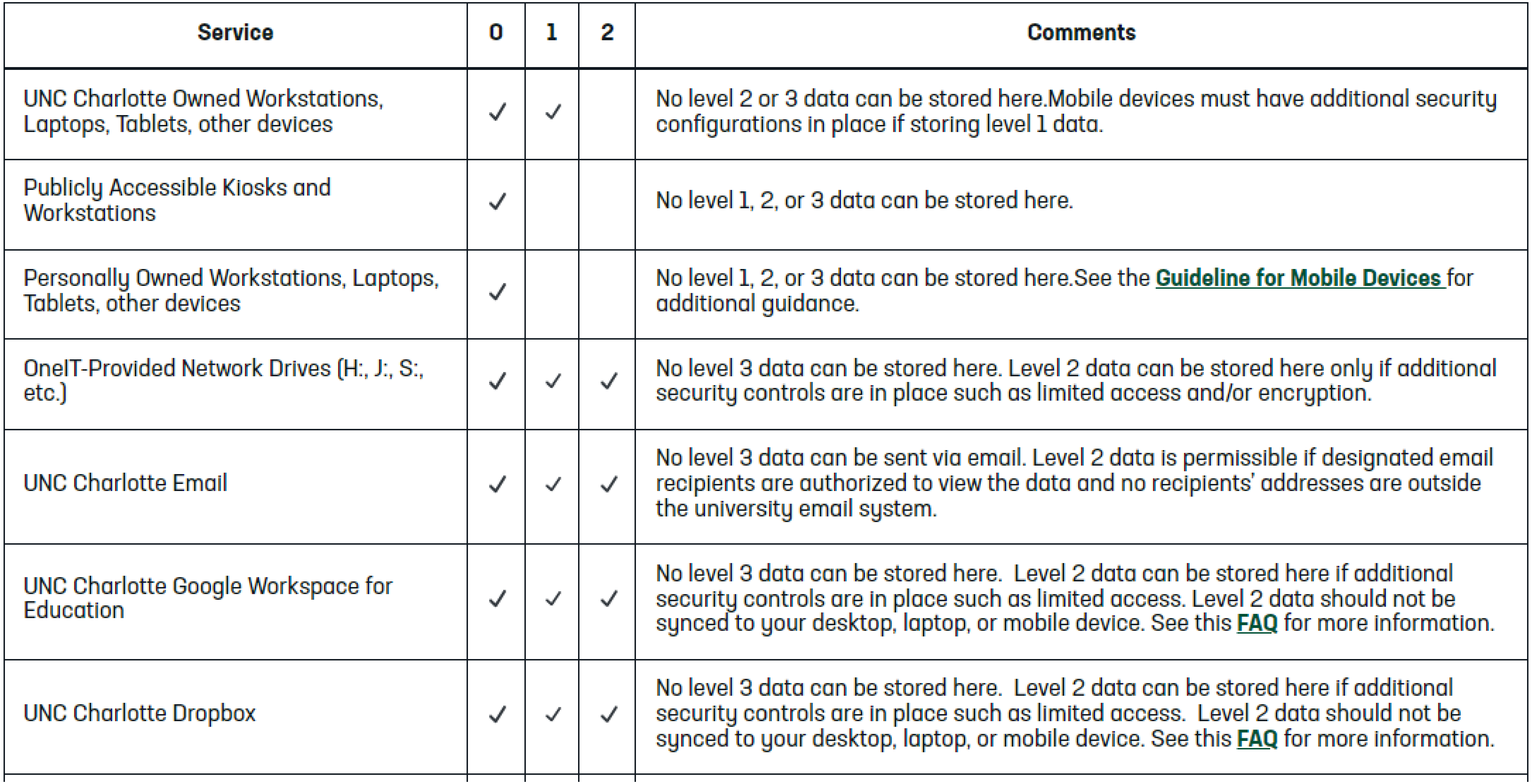
Data Handling Guideline Table

Oneit.charlotte.edu >

IT Security & Compliance >

Standards & Guidelines >

Guideline for Data Handling



Service	0	1	2	Comments
UNC Charlotte Owned Workstations, Laptops, Tablets, other devices	✓	✓		No level 2 or 3 data can be stored here.Mobile devices must have additional security configurations in place if storing level 1 data.
Publicly Accessible Kiosks and Workstations	✓			No level 1, 2, or 3 data can be stored here.
Personally Owned Workstations, Laptops, Tablets, other devices	✓			No level 1, 2, or 3 data can be stored here.See the **Guideline for Mobile Devices** for additional guidance.
OneIT-Provided Network Drives (H:, J:, S:, etc.)	✓	✓	✓	No level 3 data can be stored here. Level 2 data can be stored here only if additional security controls are in place such as limited access and/or encryption.
UNC Charlotte Email	✓	✓	✓	No level 3 data can be sent via email. Level 2 data is permissible if designated email recipients are authorized to view the data and no recipients' addresses are outside the university email system.
UNC Charlotte Google Workspace for Education	✓	✓	✓	No level 3 data can be stored here. Level 2 data can be stored here if additional security controls are in place such as limited access. Level 2 data should not be synced to your desktop, laptop, or mobile device. See this **FAQ** for more information.
UNC Charlotte Dropbox	✓	✓	✓	No level 3 data can be stored here. Level 2 data can be stored here if additional security controls are in place such as limited access. Level 2 data should not be synced to your desktop, laptop, or mobile device. See this **FAQ** for more information.

Data Classification Mistakes

Common Data Classification Mistakes

- No classification
- Misclassification
  - *Over-classification*: can lead to the implementation of unnecessary controls
  - *Under-classification*: can lead to noncompliance with data protection requirements

More Information

Office of OneIT > IT Security & Compliance > Standards & Guidelines

- Standard for Information Classification
- Guideline for Data Handling
- Guideline for Data Security in Cloud Services