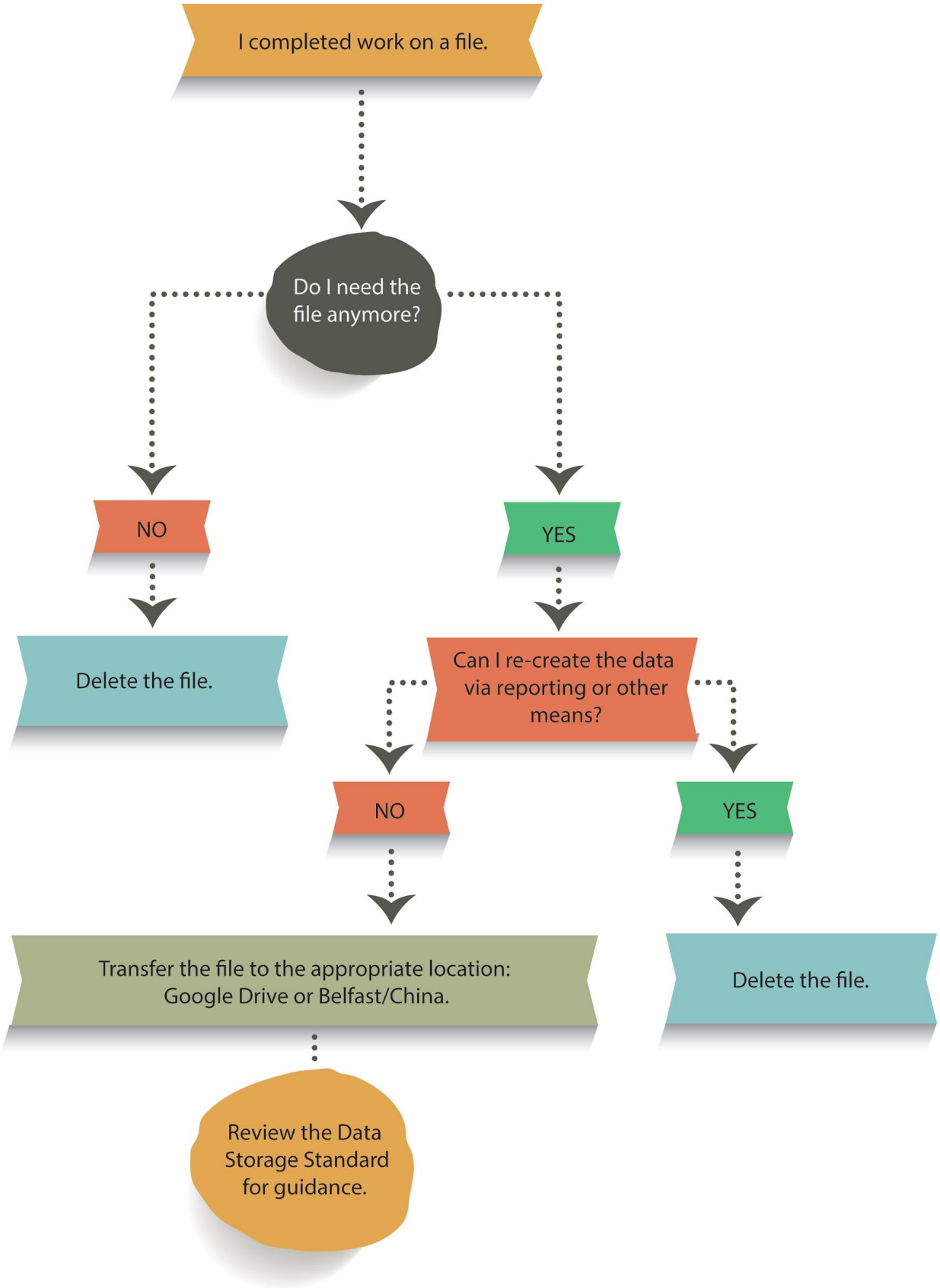
DATA WORKFLOW PROCESS | *A Data Minimization Initiative*



College Data Storage Standard

College provides two options for storing College' institutional data: Google Drive and Belfast/China. Each platform has its strengths and lends itself to particular uses. Check the table below to compare the options.

	Network Drive	Google Drive
Who's it for?	Administrative/Academic	Administrative/Academic/Students
What data types can be stored?	*Confidential - *If file has SSN or Credit Card data then it must be either deleted or modified (redacted or deleted)*	*Confidential - *If file has SSN or Credit Card data then it must be either deleted or modified (redacted or deleted)*
Where can data be accessed	On-campus or remotely via VPN	On or off-campus - and offline with Google Drive File Stream
File recovery	Yes	Yes - Information and Library Services can recover files that were permanently deleted up to approximately 25 days.
Version history	No	Yes
Use it to...	Share and/or store data that is no longer being accessed or processed on a College allocated device and/or can't be recreated at a later date. Long term archival storage - retention compliance.	Share and collaborate on any platform, inside College or outside of the College domain. Ability to sync & work offline with Google Drive File Stream.
	Belfast/China	Google Drive
Good to know...		Google allows users to change sharing permissions. ***While convenient, it poses a risk of sharing data accidentally. Be diligent in ensuring the person with whom you are sharing data has a legitimate business need.***

Data Classification Standard

Use the examples below to determine which classification is appropriate for a given type of data. When data fall into multiple categories, use the higher classification. * For reference I have included the current data classifications as set forth via the Data Governance Policy.

Public

- Institutional statistics
- academic course descriptions
- Common Data Set
- College Facts
- Information authorized to be available on College' website without requiring College authentication
- Maps, newsletters, newspapers, and magazines
- *Directory Information

**Student information contained in the College Online Directory is technically "Directory Information" under FERPA (can be released without consent) and is password protected.*

Internal

- Institutional survey data
- Enrollment projection data
- Engineering, design, and operational information about College infrastructure
- Contracts
- Unpublished research data (at data owner's discretion)
- Internal memos and email

Confidential

- Personally Identifiable Information (PII)
  - First Name, Last Name *associated with any of the following data:*
  - Social Security Number *in any form*
  - Drivers License Number and Person vehicle information
  - Passport and Visa Number
  - Account, Credit/Debit card number
  - Account passwords or personal identification number or other access codes *(when used in conjunction with First/Last name)*
  - Place/Date of birth
  - Mother's Maiden name *associated with an individual*
  - Biometric record associated with an individual: fingerprint, DNA, Iris/Retina Scan
- Protected Health Information
- Health Insurance Benefit information
  - Health insurance policy #
  - Family information all medical, SSN, PII
- Student Data
  - Student records, application, payment data
  - Financial Aid data
- College defined confidential
  - Salary Data
  - Non-public gift information

There are additional types of Confidential Data; See below

Additional Information pertaining to Personally Identifiable Information is available; see below

DATA CLASSIFICATION

Accurate classification provides the basis to apply an appropriate level of security to college data. All College data are classified into levels of sensitivity to provide a basis for understanding and managing college data. These classifications take into account the legal protections (by statute, regulation, or by the data subject's choice), contractual agreements, ethical considerations, or strategic or proprietary worth. They also consider the application of "prudent stewardship," where there is no reason to protect the data other than to reduce the possibility of harm or embarrassment to individuals or to the institution.

The classification level assigned to data will guide Data Trustees, Data Stewards, Data Administrators, and Data Users in the security protections and access authorization mechanisms appropriate for that data. Such categorization encourages the discussion and subsequent full understanding of the nature of the data being displayed or manipulated.

By default, all institutional data will be designated as "Internal." College employees will have access to the data for use in the conduct of college business.

Data Classification Levels

Public Data (low level of sensitivity)

Access to "Public" institutional data may be granted to any requester. Public data are not considered confidential. The integrity of Public data must be protected, and the appropriate owner must authorize replication of the data. Examples include: institutional statistics that appear in publications, academic course descriptions, Common Data Set, and College Facts.

* Information contained in the College Online Directory is technically "Directory Information" under FERPA (can be released without consent) but some information is password protected and should not be considered "Public."

Internal Data (moderate level of sensitivity)

This classification applies to information protected due to proprietary, ethical, or privacy considerations, even though there may not be a direct statutory, regulatory, or common-law basis for requiring this protection. Internal data is restricted to personnel designated by the College who have a legitimate business purpose for accessing such data. Examples include: institutional survey data and enrollment projection data.

Confidential Data (highest level of sensitivity)

This classification applies to information protected by statutes, policies, or regulations. This level also represents information that isn't by default protected by legal statute, but for which the Data Administrator has exercised his or her right to restrict access. Examples include: PII - Personally Identifiable Information (SSN, driver's license, bank account numbers), salary data, academic record data (unit level) and financial aid data.

Additional Types of Confidential Data:

FERPA

- Grades (including test scores, assignments, and class grades)
- Student financials, credit cards, bank accounts, wire transfers, payment history, financial aid/grants, bills

HIPAA

- Patient names, street address, city, county, zip code, telephone/FAX numbers
- Dates (except year) related to an individual, account / medical record numbers, health plan beneficiary numbers
- Any other unique identifying number, characteristic, or code

Personally Identifiable Information | Additional Information

PII is a legal concept, not a technical concept, and is not the same across the U.S. PII is a term only used in the U.S. and GDPR doesn't come right out and say what constitutes PII. They define it as: data about an identified or identifiable person, either directly or indirectly.

Personal Information does not include:

Publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media, such as:

- Phone numbers (work, home, cell)
- Street addresses (work and personal)
- Email addresses (work and personal)

It is not always the case that PII is "sensitive," and context may be taken into account in deciding whether certain PII is or is not sensitive.