Computer Data Storage and Security Policy

Purpose: To provide direction to Berea users concerning storage, protection and sharing of data belonging to the College by:

- Defining the various classes of data users need to understand when making decisions about storage, protection and sharing.
- Distributing custodianship of data to appropriate divisions and departments and establishing mechanisms for requesting and receiving permission to access and/or share data.
- Documenting the acceptable storage and management practices for each defined class of data.

Data Definition: For purposes of this policy, the term Data includes structured data records, electronic documents and any other information resources that are stored for later or ongoing reference.

Data Ownership: All data collected and stored as part of the operation of the College, and all data purchased for use in College business are the property of the College, are to be stored only on media sanctioned under this policy and are to be accessed, shared, modified or deleted only with permission of the designated data custodian or the Administrative Committee.

Data User Responsibility: Individuals who access College owned data and share it with others or store it on media to which they have access are responsible to manage the security and confidentiality of that data in accordance with College policy and all applicable government regulations. For more information about policy and regulations, contact the Compliance Committee.

Data Classes: Data classes are defined based on the type, usage, sensitivity and regulation associated with the data.

- **Personal data** – data not related to one's job or other College business.
- **Public directory data** – information about departments or individual students, faculty and staff that is publicly available via the College web site or other publication. This includes department name and primary contact phone# and e-mail address, student name and e-mail address, and staff/faculty name, job title, department, phone extension and e-mail address.
- **Individual work data** – messages, worksheets and other documents or data objects that represent College work but do not need to be stored for ongoing reference by others and are not in any of the below categories. Examples would be personal e-mails, schedules, to-do lists, and rough drafts of documents.
- **Team collaboration data** – messages, worksheets and other documents or data objects that represent the shared work of a project team, ad hoc committee or other workgroup and need to be shared among that group but do not need to be stored for ongoing reference and are not in any of the below categories. Examples would be project plans, research results and collaboratively developed documents.
- **Department/Committee data** – data objects and documents developed by a department or standing committee or other group for use within the group and possibly shared with other groups, the campus community or external collaborators, that would be considered primarily the business of the particular group, may or may not need to be stored for ongoing reference, and are not in any of the below categories. Examples would be departmental policies, calendars, work assignments, meeting minutes and procedure instructions.
- **College business data** – data objects and documents that need to be stored for ongoing reference as part of the College's business or academic records or archives. Examples would be purchase orders, student labor information, financial records, course enrollments, and student grades.
- **FERPA protected educational records** – Personally identifiable student educational records such as grades, transcripts, degree information, disciplinary records and class schedules. See https://www.berea.edu/registrar/ferpa/ for more information.
- **HIPAA protected health records** – Personally identifiable information concerning health condition, medical services or payments for medical supplies or services.
- **GLBA protected student loan records** – Personally identifiable student financial aid data or student loan

information, including payment history.

- **Sensitive research data** – Personally identifiable human subject research data containing sensitive information such as mental health, genetics, alcohol or drug abuse or illegal activities.
- **Personal identity data** – data that could be used for positive identification of an individual, such as social security number, driver license number, passport number, birth date, parent names or other data commonly used to verify personal identity.
- **Payment card data** – data that could be used to initiate unauthorized financial transactions, such as cardholder name, account number, expiration date, PIN or card verification number.
- **Export controlled research data** – data pertaining to chemical and biological agents, satellite communications, certain software or technical data, formulas for explosives or other areas controlled under ITAR or EAR regulations due to military sensitivity or other reasons.

Storage Options: The following storage options are defined for purposes of understanding and are not meant to be an exhaustive list of allowable storage options. If there is doubt about the policy concerning a particular proposed data storage or management practice, individuals should arrange consultation with IS&S data administration or management staff.

- ✓ Personal devices – Individual devices not owned by the College, e.g. home computer, personal mobile phone or personal iPad.
- ✓ Personal cloud storage – Cloud storage accounts not provisioned or administered by IS&S, e.g. Dropbox or Google Docs.
- ✓ College individual devices – Personal computers or other devices issued by the College to individual employees, e.g. laptop computer, desktop computer, iPad or mobile phone
- ✓ College individual cloud storage – Individually managed cloud storage accounts provisioned and administered by IS&S; e.g. berea.box.com individual accounts
- ✓ College group cloud storage – Cloud storage attached to a department or other group identity and managed by the group.
- ✓ College group network folders – Campus network storage attached to a department or other group identity and managed by the group.
- ✓ College software – Software or database servers or cloud software services owned or subscribed to by the College and administered by IS&S
- ✓ Departmental Software – Software or database servers or cloud software services owned or subscribed to by the College and administered by individual departments

Berea College Information Systems and Services

	Personal devices	Personal cloud storage	College individual devices	College individual cloud storage[1] (BereaBox)	College group cloud storage (BereaBox)	College group network folders	College software	Departmental Software
Personal data	**Yes**	**Yes**	No[2]	No[2]	No	No	No	No
Public directory data	**Yes**[3]	**Yes**[3]	**Yes**[3]	**Yes**[3]	**Yes**[3]	**Yes**[3]	**Yes**	**Yes**
Individual work data	No	No	**Yes**	**Yes**	No	No	No	No
Team collaboration data	No	No	No	**Yes**	**Yes**	**Yes**	No	No
Department/Committee data	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
College business data	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
FERPA protected educational records	No	No	No	No	**Yes**[4]	**Yes**[4]	**Yes**[4]	**Yes**[4]
HIPAA protected health records	No	No	No	No	No	No	**Yes**[5]	No
GLBA protected student loan records	No	No	No	No	No	**Yes**	**Yes**	No
Sensitive research data	No	No	No	No	**Yes**	**Yes**	No	No
Personal identity data	No	No	No	No	No	No	**Yes**	No
Payment card data[6]	No	No	No	No	No	No	No	No
Export controlled research data	No	No	No	No	**Yes**	**Yes**	No	No

1. Upon the ending of employment or enrollment with the College, any College individual cloud storage account attached to the departing employee or student will be immediately disabled and later deleted. Supervisors of departing employees may contact the TRC for access to individual account data.
2. The College does not take responsibility for preservation of any personal data stored on a College individual device or cloud storage account. Technical staff assisting with computer equipment repairs or upgrades will not make backup copies or data transfers of personal data.
3. Public directory data for one or a few individuals may be copied to other media such as an e-mail message or contacts folder, but publication or sharing of a copy or extract of all or a large portion of the directory is not permitted.
4. Sharing of any FERPA protected data with third parties outside the College community must be approved by the Office of the Registrar and governed by an agreement regarding appropriate usage and disclosure. See https://www.berea.edu/registrar/ferpa/ for more information.
5. HIPAA protected health records may be stored only on software and hardware specifically approved by the AC or Compliance Committee.
6. It is the College's intent to refrain from storing credit card numbers on any computer systems.