

Information Technology – Data Breach Procedure	Procedure Number	8.6.5P
	Effective Date	October 05, 2026

1.0 PURPOSE

The purpose of this document is to provide guidance on how to report suspected exposures (such as disclosures of, or unauthorized\improper access to data) or theft of College data to appropriate individuals. This document also outlines the response to a confirmed breach or theft of protected College data.

2.0 REVISION HISTORY

Adopted on: 10/05/26

3.0 DEFINITIONS

- A. *College Data* – College data are assets of The College in any form or location that meets one or more of the following criteria:
 - a. Data that The College has a legal obligation to responsibly manage.
 - b. Data that is relevant to the operations, planning, management, control, reporting, auditing, and administration of The College.
 - c. Data that is created, received, maintained, or transmitted as a result of the function of The College.
 - d. Data that is included in an official College report.
 - e. Data that is used to derive any data element that meets the above criteria.
- B. *College Protected Data* – Any data that the institution is obligated to keep private and protect from unauthorized access, including personally identifiable information, payment details, academic records, medical records, etc. The obligation to protect this data is generally outlined in a compliance standard, such as FERPA, HIPAA, GLBA, GDPR or PCI-DSS and applies to data pertaining to students as well as employees, board members, and anyone else who has data about them stored by The College, regardless of the nature of the relationship with The College.
- C. *Data* – stored collection of information that may include symbols, words, sounds or images.
- D. *Data Breach* – Any unauthorized disclosure, misuse, alteration, destruction, or other compromise of information, such as unauthorized access.
- E. *Family Educational Rights and Privacy Act (FERPA)* – A federal law enacted in 1974 that protects the privacy of student education records.
- F. *General Data Protection Regulation (GDPR)* – A comprehensive data privacy and security law created by the European Union (EU) that dictates how organizations worldwide must handle, process, and protect the personal data of EU residents.
- G. *Gramm-Leach-Bliley Act (GLBA)* – A 1999 federal law in the United States designed to regulate how financial institutions handle, disclose, and protect consumers' private financial information.
- H. *Health Insurance Portability and Accountability Act (HIPAA)* – A United States federal law designed to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

- I. *Normally Prudent Person* – An individual who exercises the level of care, judgment, and caution that a reasonable person would ordinarily use under similar circumstances, acting in good faith and based on the information reasonably available at the time.
- J. *Payment Card Industry Data Security Standard (PCI-DSS)* – A global information security standard designed to prevent credit card fraud and data breaches.
- K. *Personally Identifiable Information (PII)* – nonpublic information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to The College. Examples may include, but are not limited to, social security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information that The College has agreed to keep confidential and account passwords or encryption keys used to protect access to confidential College data.
- L. *Sensitive Information* – any information whose disclosure could cause harm to the College or its constituents including PII and proprietary information.

4.0 PROCEDURES

- A. Reporting of suspected thefts or data breaches
 - 1) Any individual who suspects that a theft, breach, or exposure of College Protected Data has occurred must immediately provide a description of what occurred via email to ITSSecurity@lccc.wy.edu, by calling 307-778-4357, or in person to a member of ITS. All reported incidents are to be logged in call tracking software, and reports of such incidents are to be delivered to the President's Cabinet each quarter.
 - 2) If a theft of physical property occurred, Campus Safety will be notified by ITS.
- B. Investigation
 - 1) ITS will investigate all reported thefts, incidents, and suspected data breaches to determine whether College Protected Data was accessed, disclosed, misused, altered, or otherwise compromised.
 - 2) While investigating such incidents, members of ITS may need to access items such as files and emails within a user account or on storage devices such as computers or removable media. This may also include personally-owned devices if such devices are found to contain College-owned data that may be involved in the reported breach.
 - 3) ITS may interview persons involved in a reported breach to gather information around the event and the nature of the data involved.
 - 4) Employees involved in potential breach incidents are expected to comply with ITS requests for information. Failure to comply with such requests may result in disciplinary action.
- C. Confirmed misuse or breach of College Protected Data
 - 1) Apart from Marketing and Communications and the President's Cabinet, College personnel are not authorized to speak on behalf of The College to media personnel or representatives of other outside agencies. All media inquiries or other public affairs inquiries should be directed to Marketing and Communications or the President's Cabinet.
 - 2) Notification Protocol

- i) If ITS determines that a breach was likely, notifications from ITS will follow what is outlined in the Incident Response Procedure 8.6.4P. Additionally, ITS must collect and share information with certain parties for the purposes outlined below.
- ii) Student Records, Financial Records, Personnel Records, and Health Records should each be evaluated to determine involvement in the reporting process. This must be done within 24 hours to meet reporting deadlines applied to certain data.
- iii) If ITS determines that the data in question is College Protected Data and that a breach is suspected, ITS must collect the following information:
 - (1) Date of the breach (known or suspected)
 - (2) Impact of the breach (number of records, number of students, etc)
 - (3) Method of breach (hack, accidental disclosure, etc.)
 - (4) Name, address, and phone number of point of contact
 - (5) Remediation status (complete, in-process, etc. with detail)
 - (6) Next steps (as needed)
- iv) This notice will be provided for:
 - (1) Data protected by FERPA or GLBA: The Director of Financial Aid for reporting to the Department of Education. GLBA requires that initial report of a breach having occurred be communicated to the Department of Education/Federal Student Aid within 24 hours of determination that a breach occurred.
 - (2) Data protected by HIPAA: The College-designated HIPAA Compliance Officer for reporting to the Department of Health and Human Services. HIPAA has different requirements for reporting a data breach:
 - (a) Individuals affected must be notified within 60 days of discovery of the breach.
 - (b) The Department of Health and Human Services must be notified within 60 days after the end of the calendar year in which the breach occurred
 - (c) If over 500 individuals were affected, HHS must be notified within 60 days of discovery and the media must also be notified within 60 days.
 - (3) Other individuals or groups as necessary.
- v) If the breach necessitates that affected individuals be notified, Marketing and Communications will manage such communications. ITS will communicate specifics of the situation to Marketing and Communications to facilitate in crafting accurate messaging around the issue.

D. Adherence

- 1) Safeguarding College Protected Data is the responsibility of all College employees. All employees are expected to safely store and handle the data that they utilize in the course of their work. Avoid storing unnecessary protected data and, when possible, redact sensitive information that is not needed for the work being done. If employees are unsure about the safety of data storage or transmission methods, please consult a supervisor or a member of ITS.
- 2) College employees must not store, upload, transfer, synchronize, or otherwise place College Protected Data on or under the control of an outside or third-party system, service, application, or storage location that has not been approved by ITS. This does not prohibit authorized access to College systems or services from a personally owned device when such access is permitted by College policy. Any use of an external system or service to store, process, or transmit College Protected Data requires written ITS

approval, except for services specifically approved by the College, including The College's Microsoft Office 365 environment.

- 3) Failure to properly maintain the data safety standards of a normally prudent person increases the institution's exposure to harm and may result in disciplinary action up to, and including, termination.

E. Appendix

- 1) Examples of events that may constitute a **Data Breach** (as defined in this procedure) include, but are not limited to, the following:
 - i) A College-owned laptop, phone, tablet, USB drive, or paper file containing College Protected Data is lost or stolen.
 - ii) College Protected Data is sent to the wrong recipient (for example, misaddressed email, incorrect mailing label, or the wrong student/employee record is shared).
 - iii) A document, spreadsheet, report, or file containing College Protected Data is inadvertently made accessible to unauthorized individuals (for example, misconfigured sharing permissions in Office 365/SharePoint/OneDrive, shared link set to "anyone," or files placed in a public-facing location).
 - iv) A user account is suspected or confirmed to be compromised (for example, phishing leading to unauthorized access, unexpected MFA prompts, or sign-ins from unusual locations) and College Protected Data may have been accessed.
 - v) Unauthorized access to a system or application containing College Protected Data (for example, an employee accesses records outside their job duties, or credentials are shared and used by another person).
 - vi) College Protected Data is stored on a non-approved third-party platform or personal device/account without ITS approval, and that data is exposed, accessed, or cannot be reliably secured or recovered.
 - vii) Malware, ransomware, or other malicious activity impacts a device or system in a way that could cause unauthorized access, alteration, or destruction of College Protected Data.
 - viii) College Protected Data is altered, deleted, or destroyed without authorization (including accidental deletion) and the integrity or availability of that data is compromised.
 - ix) Printed records containing College Protected Data are left unsecured (for example, unattended on printers, in classrooms, offices, or public areas) and may have been viewed, taken, or photographed by unauthorized persons.

Note: This list is intended to provide examples and is not exhaustive. When in doubt, report the incident as a suspected exposure or breach in accordance with Section 5(A) of this procedure.