Data Access Policy

Effective: June 2025

PURPOSE

The Data Access Policy establishes the rules and procedures by which authorized individuals obtain and use access to Pierpont ’s institutional data. The purpose of this policy is to ensure that employees, faculty, and other users have appropriate access to the data they need to perform their duties, while protecting sensitive information from unauthorized access or misuse. This policy balances the College’s responsibility to safeguard data with its commitment to operational efficiency – data security measures should not unduly interfere with the College’s business or academic processes. By defining access levels, data sharing methods, and user responsibilities, the policy aims to facilitate secure and ethical data sharing in compliance with applicable laws such as FERPA, the West Virginia Student DATA Act, and other applicable privacy regulations.

SCOPE

This policy applies to all requests for and uses of institutional data at Pierpont C&TC, regardless of the data’s format (electronic databases, cloud systems, paper records, etc.) or location. It covers all College employees, contractors, consultants, vendors, volunteers, and any other affiliates who are granted access to College data. The scope includes student educational records, employee records, financial data, research data, and any other institutional data used in official College operations. It encompasses both internal access (within the College) and external data sharing parties. All systems, applications, and computing devices that store or transmit College data are subject to this policy. Notably, this policy covers data sharing mechanisms (e.g. network file shares, email, reporting tools) and outlines secure methods for handling Personally Identifiable Information (PII) and other confidential information. It works in conjunction with the College’s information security policies and any data-sharing agreements or contracts. Where stricter requirements are imposed by law or specific agreements (such as grant data use agreements), those requirements will also apply within the framework of this policy.

POLICY

Policy Statement:
Pierpont will manage access to institutional data based on the principles of least privilege (users receive the minimum access necessary for their job) and need-to-know. The value of data as a College resource is maximized by its appropriate and widespread use, and conversely diminished by misuse, misinterpretation, or unnecessary restriction. Therefore, the College’s policy is to allow broad access to data for legitimate institutional purposes, while implementing safeguards against unauthorized access. All institutional data must be classified by a Data Steward to determine its appropriate access level, as defined in the data classification scheme below. Data designated as public may be freely accessed or released, whereas confidential and restricted data

require stringent access controls. Data access decisions will comply with FERPA (for student records confidentiality) and other applicable laws, providing that personally identifiable information is disclosed only to authorized parties or with consent, except as permitted by law. The College will protect its data assets through technical, physical, and administrative security measures and will continuously monitor access for proper use. Any individual denied access to data that they believe is needed for their role may appeal the decision to the appropriate Data Steward, Data Trustee, or Data Governance Committee for reconsideration. Ultimately, data access is a privilege and carries with it the responsibility to use data ethically, securely, and in compliance with all College policies.

Roles and Responsibilities:

Proper data access management relies on coordinated Data Governance Policy. The key roles and their specific responsibilities for data access are:

- **Data Trustee**: Data Trustees have overall accountability for who may access data in their functional area. They set high-level access policies and ensure that Data Stewards in their area are reviewing and approving access appropriately. Data Trustees resolve conflicts or gray areas regarding access (for example, if data spans multiple departments). They also ensure that institutional data access practices comply with external regulations, such as reviewing that FERPA rules are upheld in granting access to student records. Data Trustees may periodically audit or require reports on data access provisioning to verify compliance with this policy.
- **Data Steward**: Data Stewards are the primary decision-makers for access to data under their oversight. They must classify each data element or dataset (see Data Classifications below) and assign an access level. Data Stewards review requests for access: they will grant access to institutional data only to individuals with a legitimate educational or business need as defined by their job duties. That access granted is appropriate (e.g., read-only versus edit rights) and corresponds to the user's role. Data Stewards maintain records of what access has been approved and periodically re-evaluate those permissions. In addition, Data Stewards work with Data Custodians to implement any special security requirements (such as two-factor authentication for highly sensitive data) and with Data Trustees to handle any appeals of denied requests. They also enforce the Data Usage rules outlined in this policy, ensuring that data under their care is used only for approved purposes and in compliance with FERPA and other laws.
- **Data Custodian**: Data Custodians (IT administrators, database managers, etc.) implement the technical side of data access control. Upon receiving authorization from a Data Steward, Data Custodians create user accounts, set permissions, and configure system settings to grant the approved level of access. They are responsible for maintaining secure systems, including regularly updating access controls, removing access that is no longer authorized (e.g., when a user's role changes or they leave the College), and monitoring for any unusual access patterns. Data Custodians should ensure that shared data storage solutions (like network folders or collaboration tools) have proper access restrictions and encryption as needed. They also educate Data Users on secure data transfer methods (such as using encrypted email or approved file-sharing platforms) and enforce password policies and other safeguards for protecting login

credentials. If a Data Custodian discovers any unauthorized access or security breach, they must immediately report it as outlined in the incident response procedures.

- **Data User**: Data Users are individuals who have been granted access to certain institutional data to fulfill their job or academic responsibilities. Each Data User must use data only for the purpose for which access was granted and must not share their access (e.g., passwords or accounts) with others. They are expected to understand and follow all guidelines for proper data handling – for instance, not downloading sensitive data to unencrypted personal devices, not emailing unencrypted PII, and respecting any data use agreements. If a Data User is unsure whether they are authorized to use a particular data set for a new purpose, it is their responsibility to seek clarification from the relevant Data Steward. Data Users must also promptly report any data they believe to be misclassified (too open or too restricted) or any unauthorized data access they become aware of. By accepting access, Data Users acknowledge the obligation to protect the confidentiality, integrity, and privacy of the data.

Additionally, Information Technology (IT) Department staff play a support role in data access by maintaining identity management systems (such as single sign-on and directory services), auditing systems for access control effectiveness, and assisting in implementing technology for secure data sharing (e.g., secure file transfer services). The Office of Institutional Effectiveness/Research or similar units may be involved in brokering data access for reporting and analytics, ensuring such access complies with privacy rules and this policy.

Procedures or Requirements:

1. **Access Authorization Process**: Departments must follow a defined process to request access to institutional data or systems. Typically, a supervisor or department head will submit a request on behalf of a Data User, specifying the data or system and level of access needed. The request is routed to the appropriate Data Steward for approval. The Data Steward verifies the need-to-know and checks the data's classification to determine if additional approvals are required (for example, accessing confidential student data might also require FERPA training certification). Once approved, the Data Custodian (IT) provisions the access and confirms back to the requesting party. All approvals should be documented, and the principle of least privilege must be applied – e.g., granting read-only access if edit rights are not required. If a request is denied, the Data Steward will provide a reason. The requester may appeal a denial to the Data Trustee of that area, who will consult relevant policies and possibly the Data Governance Committee for a final decision.

2. **Secure Data Sharing Methods**: Whenever institutional data, especially sensitive or PII, needs to be shared between authorized users or transmitted outside the College, only approved secure methods should be used. The College provides certain tools for secure data sharing:

- *Shared Network Folders:* The IT Department can set up restricted-access network drives or SharePoint sites for departments or project teams. These shared folders are appropriate for collaborating on internal documents and can only be accessed by designated users with login authentication. Data Custodians ensure permissions on these folders are kept up to date.

- *Encrypted Email:* The College supports email encryption (e.g., using S/MIME or an email encryption gateway) for sending sensitive information. If a Data User must send PII or confidential data via email, they are required to use the College's encryption solution and follow guidelines (such as not putting PII in the subject line or body, but rather in password-protected attachments). The sender may need to coordinate with the recipient to exchange decryption information (such as a one-time passcode sent via text message).
- *Secure File Transfer and Document Management:* The College may utilize a secure document management system (such as Etrieve/SoftDocs or similar) to route and store documents containing sensitive data. These systems typically require user authentication and have audit trails for access. When sending large data files or reports, Data Users should use the College's approved secure file transfer service rather than email or personal cloud services.

All members of the College must refrain from using unapproved platforms (e.g., personal cloud storage, personal email) to share institutional data, especially if it is confidential or restricted. If there is a need for a new method of data sharing, it should be vetted and approved by the IT Department and Data Governance Committee.

3. **Data Usage Rules**: Access to data is granted for specific legitimate purposes, and any other use is prohibited. College personnel must access and use data only as required for the performance of their job functions, not for personal curiosity or gain. Data Users are categorized by their usage rights:

- *Update (Write) Access:* Only granted to users whose job duties require entering or modifying data (e.g., Registrar staff updating student records). This is tightly controlled and limited to avoid unauthorized data changes. Data Stewards grant update access based on roles, not individual preference, and ensure that users are properly trained.
- *Read-Only Access:* Most employees who need data for reference or decision-making will have view access. The College strives to grant read-only access widely when appropriate to empower employees, if such access does not risk privacy or security. Read-only access means the user cannot alter the data, only view, or download it.
- *External Data Dissemination:* Sharing institutional data with external parties—whether for regulatory reporting, research, accreditation, public relations, or any other purpose—must adhere to institutional, state, and federal guidelines, including FERPA and the College's External Data Reporting and Approval Policy.

    - Pre-Approval Requirement: All external dissemination of data must be reviewed and approved by the Office of Institutional Effectiveness (OIE) prior to release, regardless of format or audience. This includes reporting to agencies, external researchers, publishers, or the general public. No individual employee or department may release institutional data externally without OIE review, unless an explicit exemption has been granted.
    - Data Classification and FERPA Compliance:
      Only data classified as Public or defined as Directory Information under the Family Educational Rights and Privacy Act (FERPA) may be released without

individual consent. Even in these cases, the College reserves the right to restrict disclosure in alignment with individual privacy requests. Students may opt out of directory information sharing; such requests must be honored by all employees.

Any data containing personally identifiable information (PII)—including academic records, financial details, or protected demographic information—must not be released externally unless:

- Individual, informed consent has been obtained; or
- A clear legal exception under FERPA permits disclosure (e.g., to authorized government officials, financial aid providers, or for health and safety emergencies).

Any student-level data shared externally must be aggregated or de-identified, unless a valid FERPA exception applies, and OIE approval has been secured. The Data Steward(s) responsible for the data in question must also approve any such sharing when it involves non-public elements.

- Security and Access Protocols:
  As a matter of institutional and state best practices (e.g., modeled in part on WVBE Policy 4350), any external transfer of sensitive student data must follow secure data transfer protocols. Only authorized individuals should receive such data, and methods such as encryption must be used during transmission. Access to individual student records by parents or students is governed under FERPA and is managed solely through the Office of the Registrar—not through individual staff or faculty members.

4. **Data Classification Levels**: Pierpont C&TC utilizes a data classification scheme to categorize institutional data by sensitivity and to determine access control requirements. The classification levels, aligned with industry best practice definitions, are:

- *Public:* Data that may be freely disclosed to the public without risk. This includes information intended for public disclosure such as press releases, campus maps, directory information (as defined by FERPA, unless a student has opted out), and other public-facing information. Public data requires no special authorization to access, though the integrity of public data must still be protected (e.g., official published statistics should be accurate and released by authorized offices).
- *Internal*: Data meant for use within the College community that is not public but also not highly sensitive. Examples include internal memos, policies in draft, routine business records, or other information that the College prefers to keep within employees and students. Internal data should not be disclosed outside the College without permission, but access is generally open to members of the College who have a need.
- *Confidential*: Data that is sensitive and access is limited to specific groups or roles. This typically includes most FERPA-protected student education records, employee personnel records, non-public financial information, research data under confidentiality, and similar information. Confidential data should only be accessible to those in designated roles (e.g.,

an academic advisor can view their students' records, HR staff can view employee files). Unauthorized disclosure of confidential data could violate privacy laws, harm individuals, or the institution. Thus, it requires a higher level of security controls (login authentication, perhaps role-based security, etc.).

- *Restricted*: Data that is extremely sensitive, with very limited access on a strict need-to-know basis. This may include Social Security Numbers, health records covered by HIPAA, passwords or encryption keys, certain strategic plans or legal documents, and other information that, if breached, could lead to identity theft, legal liability, or significant harm. Restricted data often has additional safeguards such as encryption at rest, multi-factor authentication for access, and possibly dedicated secure environments. Only a few individuals (Data Trustees or specific designees) may have access to Restricted data, and any access or action on this data may be logged and reviewed.

Each Data Steward is responsible for classifying the data in their area into these categories. The classification must be documented (e.g., in the data inventory or next to each data element in the data dictionary). The classification then dictates handling requirements: for example, public data might be hosted on a public web server; Confidential data must be stored on secure servers and never in public repositories; Restricted data might be kept only in encrypted databases with very limited permissions. If there is uncertainty about classification, the Data Governance Committee can advise or modify definitions. Data classification will also inform how we respond to FOIA requests (Public data generally must be released if requested; Confidential/Restricted data may fall under exemptions, such as FERPA or personal privacy exemptions in WV Code).

5. **Monitoring and Review**: Access logs and data usage may be monitored by IT and Data Stewards to provide compliance. Systems that contain Confidential or Restricted data may have audit logging enabled to track who accessed what data and when. Periodically (at least annually), Data Stewards and Custodians should review user access lists for their systems (user accounts, group membership, report distribution lists) and remove or adjust access that is no longer needed. The College's Internal Audit or compliance office may conduct reviews of data access as part of broader audits. Findings from such reviews might include over-privileged accounts, unused accounts, or potential segregation of duties issues (e.g., someone who can both enter and approve a transaction) – these should be corrected under the guidance of Data Trustees.

6. **Consequences for Unauthorized Access or Misuse**: Any person who accesses data without proper authorization, or misuses data (for example, by exceeding their authorized access, sharing confidential data with unauthorized parties, or using data for personal gain or malice) is in violation of this policy. As soon as such an incident is identified, it should be reported as a security incident. The College will follow its incident response procedures, which may involve the IT security team and possibly law enforcement if laws are broken. Consequences may include immediate termination of access pending investigation, and, if confirmed, could lead to disciplinary action up to termination and legal action. The Consequence of Noncompliance with data usage rules is serious: violators may be subject to College conduct code penalties, up to and including discharge, and even civil or criminal penalties under laws like FERPA (which can lead to federal action). In less severe cases (e.g., accidental minor breaches), the College may require re-training and a reaffirmation of the individual's understanding of data policies, or temporarily suspend access.

Compliance and Enforcement:

Compliance with the Data Access Policy is mandatory for all individuals covered under the Scope. Pierpont will enforce this policy through oversight and technical controls. Data Custodians will implement system-enforced access controls that align with the policy, and any attempt to circumvent such controls (hacking, using another's credentials, etc.) is prohibited and subject to discipline, up to and including discharge. Data Stewards and supervisors are responsible for ensuring that their staff complete required training and follow procedures when requesting or using data access.

The College will utilize compliance checks, such as quarterly reviews of high-risk data access or reports from security tools that highlight policy violations (for instance, alerts if someone emails a file with Social Security numbers in plain text). Unannounced audits may be conducted on user activity for systems containing sensitive data to verify that usage aligns with job functions.

Enforcement actions for non-compliance with this policy can include:

- Revocation of access rights, either temporary or permanent, to prevent further unauthorized activity.
- Mandatory security or privacy training for those who violate guidelines unintentionally or due to lack of understanding.
- Disciplinary measures in accordance with College HR policies or student conduct codes. This might range from a written warning up to termination of employment or student expulsion, depending on severity and whether it is a repeat offense.
- Legal action or reporting to law enforcement in cases of unlawful data breaches. For example, willful disclosure of confidential student information without authorization could violate FERPA; the College would report such incidents to the U.S. Department of Education and could face sanctions, and the individual could face legal consequences. Similarly, computer misuse might violate state or federal computer crime laws.

If a data breach or incident occurs related to unauthorized access, enforcement will also mean executing the incident response plan – containing the incident, notifying affected individuals (for example, if a breach exposes student PII, we would notify those students in line with state policy which expects prompt notification to parents or students after a breach, and possibly notifying state authorities (the WV Attorney General or Governor's office, as applicable, for significant breaches as suggested in WV Code §18-2-5h for WVDE-level incidents). The College will take corrective actions post-incident, which are part of enforcement to prevent future violations.

Ultimately, every user's adherence to this policy is critical. By signing College employment or access agreements, users acknowledge their responsibility to follow this Data Access Policy. Willful or negligent non-compliance will be addressed firmly to protect the College's data assets and maintain trust with our students, employees, and other stakeholders.

Related Documents and References:

- Pierpont Data Governance Policy
- Pierpont Data Integrity Policy

- Family Educational Rights and Privacy Act (FERPA)
- West Virginia Freedom of Information Act (WV FOIA), W. Va. Code 29B-1-1 et seq.
- Pierpont Information Security Policy
- Pierpont Incident Response Plan