Data Governance Policy

Effective: June 2025

PURPOSE

The Data Governance Policy establishes a framework for managing Pierpont Community & Technical College's institutional data as a strategic asset. Its purpose is to ensure that data is handled in a consistent, secure, and responsible manner. This policy promotes freedom of access to data by all members of the community while enforcing compliance with all applicable laws and regulations. By defining roles, responsibilities, and procedures for data governance, the College aims to enhance data quality, integrity, and availability for decision-making and operational efficiency.

SCOPE

This policy applies to all institutional data maintained by Pierpont C&TC, whether stored electronically or in paper format. It covers all College departments and units, and all employees, contractors, vendors, or agents, managing or using College data. Institutional data includes any information related to College operations (e.g., student records, employee data, financial and administrative data) that meets one or more of the following criteria: (1) data required for integration across systems or key to institutional processes; (2) data needed to meet internal or external reporting requirements; (3) data used in official College reports; or (4) data required by a broad cross-section of users. This policy is aligned with federal and state requirements, including the Family Educational Rights and Privacy Act (FERPA) and relevant West Virginia laws. In cases where other policies (e.g., IT security policies) overlap with data governance, all applicable policies shall be followed.

POLICY

Policy Statement:

Pierpont C&TC is committed to strategic and effective decision-making regarding its information assets through formal data governance. All institutional data will be managed according to defined standards of security, privacy, quality, and accessibility. The College adopts a philosophy that institutional data should be accessible to authorized individuals for legitimate educational and business purposes, coupled with a duty to protect sensitive information in compliance with FERPA and other privacy laws. Data governance decisions will be made transparently and documented appropriately. Every data element will be classified (e.g., Public, Internal, Confidential, Restricted) and given an appropriate security level by the responsible Data Steward. Data policies and procedures will be coordinated College-wide, ensuring consistent interpretation across systems and proper safeguards for data throughout its lifecycle. Any new systems or processes involving institutional data must adhere to this policy and receive approval through the data governance framework.

Roles and Responsibilities:

Effective data governance requires clearly defined roles. The following roles are responsible for implementing and enforcing this policy:

- **Data Trustee**: A senior College official accountable for oversight of data governance in their functional area. Data Trustees are responsible for the security, privacy, and quality of institutional data, and for ensuring compliance with data management policies and standards. They work with Information Technology, Institutional Effectiveness, and other stakeholders to allocate resources (staff, technology) to support data needs across the College. Data Trustees coordinate campus-wide data governance efforts, define the overall structure of data stewardship, and chair the Data Governance Committee or equivalent. They also promote data-informed decision making and ensure that critical data assets (student, financial, human resources data, etc.) have defined stewardship. Data Trustees make or approve strategic decisions about data policies and resolve conflicts or issues escalated by Data Stewards.
- **Data Steward**: A functional area manager or subject-matter expert assigned by a Data Trustee to oversee specific data sets or domains (e.g., student records, HR, finance, academic affairs). Data Stewards implement and enforce data policies and procedures within their area. They are responsible for classifying data elements under their care, defining data definitions, and ensuring data accuracy and consistency. Data Stewards approve or deny requests for access to data within their domain in accordance with this policy and FERPA guidelines. Their responsibilities include completing data governance and classification training, identifying all major data systems and repositories for their domain, and appointing Data Custodians for technical management. They must safeguard data from unauthorized access or alteration and authorize data use only for legitimate purposes. Data Stewards also meet regularly (for example, as a Data Governance Committee) to review data issues, coordinate data definitions, and plan for data needs across the College.
- **Data Custodian**: An IT or operations staff member (such as a database administrator, system administrator, or security officer) responsible for the technical environment and day-to-day management of institutional data systems. Data Custodians maintain systems housing institutional data and enforce access controls as specified by Data Stewards. Their duties include implementing backup and recovery procedures, monitoring system security, and applying data protection measures (encryption, user authentication, etc.). Data Custodians process authorized requests for adding, modifying, or removing user access, ensuring that access permissions align with the Data Steward's approvals. They document and uphold operational standards and procedures for data handling, and work with Data Stewards to update procedures as needed. In addition, Data Custodians are involved in technical aspects of data integrity, such as maintaining data integration between systems and preventing data loss or corruption.
- **Data User**: Any individual (faculty, staff, contractor, or other authorized agent) who accesses or uses institutional data to perform their job functions or academic responsibilities. Data Users are only granted access to the data necessary for their role ("need-to-know" basis) and must use data solely for official College business purposes. They are expected to understand and adhere to all relevant data policies, including privacy and security requirements. Data Users must protect any confidential information

they access and report any suspected data issues or incidents to the appropriate Data Custodian or Steward. They do not own the data they use; rather, they act as custodians of the information on behalf of the College and are accountable for using it ethically and legally.

All members of the College community have a shared responsibility to ensure data is handled properly. Information Technology (IT) personnel support the data governance process by providing the infrastructure and tools for secure data storage, sharing, and backup, and by assisting Data Trustees and Stewards in technical implementation of data standards. The Office of Institutional Effectiveness also plays a key role by facilitating data-informed decision-making, promoting data quality, and supporting institutional research efforts aligned with governance standards. If any questions arise regarding roles, the Data Trustee for the area or the College's executive leadership will clarify responsibilities.

Procedures or Requirements:

Data Governance Structure: Pierpont C&TC will maintain a Data Governance Committee or similar committee comprised of Data Trustees and Data Stewards from key functional areas (e.g., academics, student services, finance, IT, human resources). This committee will meet regularly (e.g., monthly) to discuss data-related issues, approve data standards, and review compliance with data policies. Meeting agendas and decisions will be documented. The committee is responsible for reviewing any new institutional data collections or proposed changes to data systems to ensure alignment with governance standards.

Data Classification: As part of governance procedures, every institutional data element must be assigned a classification level by the relevant Data Steward, in line with the College's Data Access Policy. The categories generally include Public, Internal, Confidential, and Restricted, as defined in the Data Access Policy (see Related Documents). Classification determines the security controls and access permissions required for that data. Data Stewards should maintain an inventory or data dictionary of the data elements under their purview, including definitions and classification of each element. In accordance with West Virginia's Student DATA Act principles, the College will document data elements and their purposes, and make publicly available a high-level inventory of the types of student and institutional data collected, where appropriate. This inventory will not include any sensitive personally identifiable information but will improve transparency of our data practices.

Data Standards and Quality: Data Stewards, in consultation with Data Trustees, will define standards for data entry, naming conventions, and metadata for their areas to ensure consistency across systems. Key data elements that are shared across multiple systems (for example, student ID numbers, course codes, employee IDs) must be consistent and synchronized. The College will maintain a central repository of metadata (data about data) for core institutional data. This metadata will include technical definitions, valid values, and business rules for each data element. For example, if "full-time enrollment" is a data element, the repository would describe how it's calculated, the term definitions, and any timing considerations (such as census dates). Adhering to these standards is mandatory; any changes to core data definitions must be reviewed by the Data Governance Committee.

Access and Authorization Procedures: All requests for access to institutional data (beyond what a user is automatically granted by virtue of their role) must follow formal procedures. Typically, a Data User's supervisor or department head will request access for the user to specific systems or reports. The appropriate Data Steward will review the request to ensure it aligns with the user's job responsibilities and the data's classification. Approved requests are then implemented by Data Custodians, who will grant the minimum necessary access privileges. Data Trustees and Stewards will periodically review user access lists to verify that access remains appropriate and revoke any access that is no longer needed (for example, when an employee changes roles or leaves the College). If a Data Steward denies a request for access, that decision can be appealed to the Data Trustee or the Data Governance Committee for further review.

Training and Awareness: All individuals with roles in data governance (Trustees, Stewards, Custodians, and Users) must undergo training relevant to their responsibilities. Data Trustees and Stewards should receive training in data stewardship, classification, FERPA compliance, and relevant privacy/security laws. Data Users must receive basic training on data security, privacy, and proper data usage. The College will also provide periodic awareness programs about data governance policies, updates on any changes in laws (such as FERPA regulations or state privacy laws), and guidance on ethical data practices. Compliance with training requirements is considered part of each role's duties.

Incident Reporting and Response: In the event of any suspected or actual data breach, unauthorized disclosure, or significant data error, it must be reported immediately to the appropriate authority (e.g., the IT security office, Data Custodian, or Data Trustee). The College will follow the West Virginia Higher Education Policy Commission's Privacy Management and Incident Response Plan, which provides procedures for containing and managing data breaches. This includes classifying the incident, notifying affected parties in accordance with state law, and mitigating any damage. Under West Virginia's Student Data Act, the College is mindful of the expectation to notify authorities and individuals of breaches involving personally identifiable information. Pierpont C&TC will ensure timely notification to affected students or employees if their confidential data is compromised, consistent with state and federal guidelines. After an incident, the Data Governance Committee will review the incident to identify lessons learned and recommend improvements to policies or practices to prevent future occurrences.

Compliance and Enforcement:

All College community members must comply with the Data Governance Policy. Failure to adhere to this policy may result in disciplinary action as per College procedures or employment agreements. Specifically, employees or students who violate data governance standards – for example, by accessing data without authorization, mishandling sensitive information, or failing to follow required procedures – will be subject to investigation. Minor or inadvertent violations may be addressed through remedial training and temporary suspension of access; serious or willful non-compliance can result in formal discipline up to termination of employment or dismissal from the College and may carry legal consequences if laws (such as FERPA or data protection laws) are violated. Data Trustees are responsible for overseeing compliance in their areas and ensuring that any compliance issues are corrected. The College's executive leadership

(or a designated compliance officer) may conduct periodic audits or reviews of data handling practices to ensure this policy is followed.

The College also recognizes the West Virginia Freedom of Information Act (WV FOIA) as a legal framework governing public access to records. While many educational records are protected by privacy laws and thus exempt from disclosure, the College will respond to FOIA requests in compliance with W. Va. Code §29B-1-1 et seq., ensuring that any release of records is reviewed by the appropriate Data Trustee and the College's legal counsel. Public records (as defined by law) will be provided upon valid request, whereas confidential student or personnel data will be withheld or redacted according to legal exemptions (e.g., FERPA-protected information). Any willful violation of FOIA or wrongful withholding of public records can result in penalties, so the College will balance transparency with privacy compliance diligently.

Adherence to this policy will be enforced by the Data Governance Committee and the College administration. Enforcement mechanisms include requiring remediation plans for units found non-compliant, removing, or limiting access for individuals until compliance is assured, and reporting serious breaches to senior administration or regulators as required. All College personnel are expected to report any suspected violations of this policy to their supervisor, a Data Steward, or anonymously through any established ethics or compliance reporting structure. Reports of non-compliance will be reviewed confidentially and without retaliation.

Related Documents and References:

- Pierpont C&TC Data Access Policy
- Pierpont C&TC Data Integrity Policy
- Family Educational Rights and Privacy Act (FERPA)
- West Virginia Freedom of Information Act, W. Va. Code §29B-1-1 et seq.
- WV Code §18-2-5h: Student Data Accessibility, Transparency and Accountability Act
- WV Board of Education Policy 4350
- WV Higher Education Policy Commission – Privacy Management and Incident Response Plan
- WVDE Data Access and Management Guidance