Data Integrity Policy

Effective: June 2025

PURPOSE

The Data Integrity Policy is intended to ensure that Pierpont Community & Technical College's data is valid, reliable, consistent, and accurate across all systems and uses. The purpose of this policy is to uphold a high degree of integrity for the College's sensitive data so that faculty, staff, administrators, and decision-makers can trust the information for operational needs and strategic planning. By establishing standards for data definition, documentation, and quality control, and by clarifying responsibilities for maintaining data integrity, the College seeks to enable effective data integration across functional units and information systems. This policy also supports compliance with internal and external reporting requirements, ensuring that reports to state and federal agencies (and to the public) are based on consistent and correct data. Ultimately, the Data Integrity Policy helps protect the College's credibility and decision-making by preventing data errors and inconsistencies.

SCOPE

This policy applies to all institutional data defined in the Data Governance Policy and used by Pierpont C&TC. It covers all systems that store College data (student information systems, finance systems, learning management systems, etc.) and all personnel who enter, manage, or utilize data. The scope includes:

- **Data Entry and Capture:** How data is initially collected or input into College systems (e.g., admission forms, employee onboarding data, grade entry).
- **Data Maintenance:** Ongoing processes that update or modify data (e.g., changes to addresses, program curriculum updates, financial transaction entries).
- **Data Integration:** Transfer or synchronization of data between systems (e.g., syncing of student IDs between registration system and library system) and aggregation of data for reporting.
- **Data Reporting and Use:** Generation of reports, analytics, and decision-support information that rely on underlying data being consistent and well-defined.

All departments and units of the College are within scope, including any third parties or contractors who manage College data (such as a vendor managing a cloud-based system containing College records). If any data is shared with or reported to external entities (like the WV Community and Technical College System office, federal IPEDS reports, accreditation bodies), this policy ensures that such data has integrity from the point of origin. The policy particularly addresses "core data elements" that are used widely, such as student IDs, course codes, financial account codes, etc., because these must be consistent across all platforms. Note that while this policy focuses on accuracy and consistency (quality of data), issues of data confidentiality or access are covered in the Data Access Policy. However, some overlap exists (e.g., correcting a data error might involve access to correct it). In case of any conflict, data integrity should be maintained without violating access rules (meaning corrections should be

done by authorized persons). This policy is aligned with **WVBE Policy 4350** and other guidelines to ensure that when we collect and maintain student data, we follow standardized definitions and procedures to keep that data accurate and meaningful.

POLICY

Policy Statement:

Pierpont C&TC asserts that institutional data must be consistently defined and understood, and that data values are to be correct and trustworthy. Data integrity refers to the accuracy, completeness, and reliability of data over its lifecycle. The College will establish and enforce standards such that key data elements have the same meaning across different departments and systems. For example, terms like "full-time student," "faculty FTE," or "operating expenditure" will have one official definition used College-wide for all reporting purposes. All College data systems should be designed and maintained to incorporate these standard definitions and acceptable value ranges. Each Data Steward is responsible for the correctness of data values within their area of responsibility, which means they must put in place processes to prevent and detect errors. The Information Technology department will support the integrity of data by ensuring technical consistency (such as referential integrity constraints in databases, removal of duplicate records, and accurate synchronization between systems). The IT Department will ensure that the needs of data users are considered when designing or modifying data structures, so that systems support correct and meaningful data capture. When institutional data is used for official reporting or decision-making, it must come from the authoritative sources defined by the College's data governance framework (for example, official enrollment numbers should come from the student information system after census date to guarantee consistency). Any transformation or aggregation of data for reporting must preserve accuracy and be documented. In summary, College data will be consistently interpreted across all College systems according to best practices agreed upon by Data Stewards, with documented definitions and values. Where discrepancies or errors are discovered, the College is committed to correcting them at the source and communicating the corrections to all stakeholders who use that data.

Policies and Responsibilities:

Maintaining data integrity is a shared responsibility, but specific roles have the following duties:

- Data Trustee: Data Trustees have leadership responsibility for data integrity in their respective areas. They ensure that adequate resources and attention are given to data quality. This can include sponsoring data cleanup projects, approving data quality tools or software, and ensuring cross-department cooperation. Data Trustees work with Data Stewards to set priorities for improving data (for instance, deciding to standardize a particular data element College-wide). They also arbitrate any conflicts in data definitions or usage between departments. If external reporting issues arise (e.g., a state report uncovered inconsistent numbers), Data Trustees coordinate the response and remediation plan. They promote a culture that values accuracy over convenience – for example, encouraging staff to take the time to enter data correctly and to verify information. Data

Trustees may also be involved in approving any exceptions to data standards when a unique situation occurs.

- Data Steward: Data Stewards are the front-line managers of data integrity. For each key data element in their domain, they must ensure a clear definition exists and that it is used uniformly. They document these definitions and business rules in the College's data dictionary or metadata repository. Data Stewards establish procedures for data entry and maintenance that uphold integrity (for example, requiring dual review of critical data entries, or setting validation rules such as allowable value ranges for certain fields). They are responsible for conducting periodic data quality audits within their area – this might include running reports to find missing or anomalous values (like students without a birthdate on file, or courses with zero credits) and correcting them. Data Stewards also collaborate with one another for data that crosses functional areas; for instance, the Registrar (student data steward) and the Financial Aid Director (financial aid data steward) might coordinate to ensure that a student's enrollment status is consistently recorded for both academic and aid purposes. If Data Stewards identify systemic issues (e.g., a form is collecting data incorrectly, or users are misunderstanding a definition), they can recommend changes to processes or systems. It is ultimately the responsibility of each Data Steward to ensure the correctness of the data values for the elements within their charge, meaning they take ownership of data quality in their domain.

- Data Custodian: Data Custodians have technical responsibilities that significantly impact data integrity. They implement and maintain technical controls such as data validation rules in software, database constraints (like primary/foreign keys to enforce referential integrity between related records), and automated checks that prevent obviously bad data (for example, preventing an invalid date or an out-of-range value from being entered). Data Custodians performing data integrations between systems (such as importing data from one system to another) must ensure that mappings are correct and that no data is lost or mis-translated in the process. They should create or utilize scripts to identify duplicate records or inconsistencies (for example, two IDs for the same person) and work with Data Stewards to resolve them. Backups and disaster recovery plans are also within the purview of Data Custodians – while these are often seen as security measures, they are crucial for integrity, as they allow restoration of correct data in the event of data loss or corruption. Data Custodians must make sure that when systems are upgraded or patched, data integrity is preserved (e.g., by testing that reports still produce the same results after a system change). If a Data Custodian notices unusual data issues (like a sudden surge in errors or missing data fields), they should alert the Data Steward and investigate the root cause (which could be a technical glitch or a user process issue).

- Data User: All Data Users, especially those who enter or update data, play a vital role in maintaining integrity. They must follow the procedures and data standards provided to them – for example, using the proper format for names, entering data in the correct fields, and not bypassing required fields. Data Users should double-check their work when inputting critical data and are encouraged to ask for clarification if they encounter ambiguous cases. Just as important, Data Users are expected to be vigilant for potential errors or inconsistencies. If a Data User discovers what they believe to be incorrect data

(such as a report that shows implausible numbers, or a student record that seems wrong), they should report it to the appropriate Data Steward or their supervisor. All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate Data Steward or the Data Trustee. This means Data Users have a responsibility not to ignore data issues; reporting and fixing small errors can prevent larger issues down the line. In addition, some Data Users (like analysts or report writers) may be tasked with combining data from multiple sources – they must do so using the official definitions and ensure they aren't inadvertently creating inconsistencies (for instance, by using unofficial data from a spreadsheet that conflicts with official system data).

Everyone in the College community must understand that data integrity is foundational – without accurate data, the analyses or decisions based on that data will be flawed. Therefore, each role from Trustees to end-users must perform their duties with care for data quality.

Procedures or Requirements:

To enforce data integrity, the College sets forth the following procedures and requirements:

1. Data Definition and Documentation (Metadata): The College will maintain a data dictionary or metadata repository for key institutional data elements. The Data Trustee (or a designated Data Steward) will oversee this repository. Each entry in the data dictionary will include: the data element name, a clear definition, the owner (Data Steward) responsible, the system of record (where it primarily resides), acceptable values or format, and any business rules (e.g., how it's derived, update frequency, and applicable date ranges). For example, an entry might define "Student Credit Hours" and specify how it's calculated and in what context (term, session) it's valid. This documentation should be available to all Data Users (at least those with relevant access) so they can consistently interpret the data. When new data elements are introduced (such as a new field in a system or a new report metric), they must be defined and added to the dictionary. Likewise, if any data element's definition is changed, the change must be approved by the Data Governance Committee and updated in the documentation. This practice aligns with the Student Data Accessibility and Transparency Act requirements for having a data inventory and definitions for elements, promoting transparency and clarity.

2. Data Input Controls: Departments must follow standardized procedures for entering and updating data. These procedures can include using official forms (physical or electronic) that have built-in validations, following an approval workflow for certain changes (e.g., grade changes might require approval, budget transfers might require dual authorization), and adhering to timelines (for instance, ensuring that all data for a semester is entered by a certain cutoff date for reporting). The IT systems will enforce many low-level validations (like not allowing letters in a numeric field, or requiring mandatory fields). Beyond that, Data Stewards should identify critical data fields that require extra verification. For example, when entering a new student record, an admissions officer might be required to verify the Social Security Number against existing records to avoid duplicates. Training will be provided to data entry personnel on common errors to avoid

and the importance of accuracy. In cases where data originates from an external source (like standardized test scores from a testing agency), procedures should ensure that the data is imported accurately and that any conversion or matching to internal records is done correctly (for instance, matching test scores to the right student).

3. Data Quality Monitoring: The College will implement routine data quality checks. These checks can be automated or manual. Examples include:
    - Data Audit Reports: Scheduled reports that look for anomalies, such as duplicate IDs, null values in fields that should always be populated, out-of-range values, or inconsistent data between systems (e.g., a student marked "graduated" in one system but still "active" in another).
    - Reconciliation Processes: Regular reconciliation between related systems. For instance, the Business Office and Financial Aid Office might reconcile financial records to ensure that student charges in the billing system match the records in the student information system. Similarly, HR data in the payroll system might be reconciled with data in a personnel system.
    - Key Performance Indicators (KPIs) for Data Quality: The Data Governance Committee may define metrics like "error rate in data entry" or "percentage of records with complete information" and monitor these over time. If a department has a high error rate, additional training or process changes can be implemented.

Data Stewards will review quality reports and coordinate data cleansing efforts when needed. Data cleansing might involve correcting data in bulk (with careful oversight) or one-by-one fixes for unique cases. Any systematic issues discovered (like a certain field frequently being left blank due to a form design problem) should be addressed by changing the process or system.

4. Change Management for Data Structures: When changes to data structures are proposed (such as adding a new field, changing a code value set, or redesigning a database), a change management process must be followed to ensure data integrity is maintained. This involves:
    - Impact Analysis: Assessing how the change will affect existing data and reports. For example, if a new student type code is introduced, how will it impact enrollment reports or downstream systems that consume that code?
    - Data Conversion or Migration: If data needs to be converted (e.g., splitting one field into two, or merging codes), a plan must be developed to transform the old data to the new structure without loss of meaning. Data Custodians would run conversion scripts or manual updates, and Data Stewards would verify a sample of records for correctness post-conversion.
    - Testing: Before changes go live, they should be tested in a non-production environment with real or realistic data to catch any issues. Key reports should be run to ensure they still work and produce expected results with the new changes.
    - Approval: Significant changes should be reviewed by the Data Governance Committee or at least the relevant Data Trustee and Steward to ensure the changes align with data standards. They must update the data dictionary if definitions or acceptable values change.

By managing changes carefully, the College prevents unintended data corruption or inconsistency that can occur when systems or business processes change.

5. Data Integration and System Alignment: The College will maintain a single logical data model or an enterprise architecture plan that maps how data in one system relates to data in another. Practically, this means identifying systems of record for each data domain (for instance, the HR system is the system of record for employee data, the Student Information System for student enrollment, etc.) and ensuring other systems either pull from those sources or update back to them. Interfaces and data feeds between systems should be timely and reliable. If multiple systems hold the same data element, one is designated authoritative and updates flow from it to the others. Data Custodians and Stewards should meet to discuss any discrepancies that arise between systems and correct them. The goal is that a data point (say a student's status or a faculty member's title) is the same in every system that uses it. This reduces confusion and errors when reports combine data. In support of the WV State data integration goals, our policy ensures that any data reported to the state or federal level is drawn from integrated, consistent sources so that, for example, enrollment numbers reported to the WV Higher Education Policy Commission match those in our internal reports and IPEDS submissions.

6. Issue Resolution and Continuous Improvement: When data issues are reported by Data Users or identified through audits, the College will address them systematically. Minor, isolated errors will be corrected by the responsible Data Steward or Data Custodian. For more widespread issues, a data integrity task force or the Data Governance Committee may form a project to clean and correct the data. The steps typically include identifying all affected records, determining the correct values (which may involve research and cross-checking sources), updating the data (preferably through controlled scripts or tools to avoid manual error), and confirming the fix. After resolution, the team should analyze why the issue occurred and implement safeguards to prevent it from recurring. For example, if a batch of student records had incorrect program codes due to a manual entry mistake, the solution might include adding a dropdown menu for that field to avoid typos. All employees are encouraged to provide suggestions to improve data processes, and these suggestions will be reviewed.

Additionally, incident response for data integrity overlaps with security incident response when data integrity is compromised maliciously (e.g., unauthorized alteration of records). In such cases, incident response procedures (like those in the Privacy Incident Response Plan) will be invoked to investigate and recover the correct data state, including restoring from backups if necessary. The College will ensure that breach planning and mitigation not only considers confidentiality but also the integrity and availability of data. If any data integrity issue rises to the level of impacting report accuracy externally (such as a published report with errors), the College will issue corrections and notify stakeholders as appropriate.

Compliance and Enforcements:

All College personnel and units must comply with the Data Integrity Policy. Given that data integrity lapses can be unintentional, the College's approach to enforcement emphasizes prevention and correction over punishment. However, willful neglect or manipulation of data will face strict consequences. For instance, knowingly falsifying data in a College record (such as altering a student's grade or misreporting financial figures) is a serious offense that could lead to disciplinary action including termination and referrals for academic or legal consequences as applicable.

Accountability: Data Stewards are accountable for monitoring compliance within their domains. If a department or user is repeatedly responsible for data errors, the Data Steward (with support from the Data Trustee) may require additional training or process changes in that department. Supervisors should treat data accuracy as part of job performance for employees who handle data extensively. The Office of Institutional Research or a similar body may periodically review data submissions for accuracy and report any concerns to Data Stewards and Trustees.

Auditing and Review: The College may conduct audits of data integrity, possibly in conjunction with internal audit or external auditors (for example, auditing the accuracy of data submitted in accreditation reports or financial statements). Any audit findings related to data inconsistencies must be addressed with a formal action plan. Data Trustees will ensure that these plans are executed, which might include data cleanup or improved controls.

Enforcement Actions: In the event of non-compliance that jeopardizes data integrity, several actions can be taken:

- If an individual is found to be careless or not following procedures (e.g., bypassing validations or ignoring the required process), their data access may be suspended until they are retrained. Persistent failure to follow data integrity procedures can lead to HR disciplinary processes.
- If a particular system or process is identified as a weak link (for example, a legacy system that cannot enforce needed rules), the College will prioritize it for upgrade or replacement. Interim measures (like extra manual checks) will be enforced.
- In cases of academic or research data, if integrity is compromised (for instance, a research dataset is mishandled), the incident might be referred to academic integrity or research compliance offices for additional review, given that it could overlap with research misconduct policies.

The College also aligns this policy with state and federal compliance requirements. For instance, the WV Student DATA Act implies routine compliance audits for privacy and security which can encompass data integrity checks as well. The College will include data integrity verification as part of ensuring FERPA compliance – e.g., verifying that data reported out under FERPA exceptions (like health/safety emergencies or studies) is accurate and goes to the right recipients. Under WVBE Policy 4350, educational institutions must maintain procedures for data quality when collecting and reporting student data; while Pierpont C&TC is a higher ed institution, we strive to meet similar standards by documenting how data is collected and ensuring it remains accurate through its use.

Incident Consequences: If poor data integrity leads to a significant incident (like incorrect data sent in an official report or a breach of data accuracy due to a security incident), the College will analyze the root cause and enforce any needed accountability. This might mean revising this policy, updating training, or in severe negligence cases, holding responsible parties accountable. A data breach that corrupts data (as opposed to exposing it) is still a breach; the College would follow the incident response plan to restore correct data and possibly involve law enforcement if malicious tampering occurred.

All employees and students are reminded that maintaining data integrity is part of our ethical responsibility. The College's Code of Conduct (or equivalent) covers honesty and accuracy in record-keeping. Therefore, compliance with this Data Integrity Policy is not just an IT or administrative requirement, but a fundamental part of each community member's duty. The College will enforce this through both technical means and community standards, ensuring that our institutional data can be relied upon with confidence.

Related Documents and References:

- Pierpont C&TC Data Governance Policy
- Pierpont C&TC Data Access Policy
- WV Code §18-2-5h (Student DATA Act)
- WV Board of Education Policy 4350
- Family Educational Rights and Privacy Act (FERPA)
- Institutional Data Dictionary/Metadata Repository
- WV Higher Education Privacy and Incident Response Plan