GLB COMPLIANCE POLICY

OBJECTIVES

1. Ensure security & confidentiality of customer information
2. Protect against anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

KEY ELEMENTS

1. Designate an employee to coordinate the institution's information security program
2. Identify reasonably foreseeable internal & external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of an institution's operations, including:
    a. Employee training & management
    b. Information systems, including network & software design, as well as information processing, storage, transmission, & disposal; and
    c. Detecting, preventing, & responding to attacks, intrusions, or other system failures.
3. Design & implement information safeguards to control the risks identified through the risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguard's key controls, systems, & procedures.
4. Oversee service providers, by:
    a. Taking reasonable steps to select & retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
    b. Requiring service providers by contract to implement & maintain safeguards.
5. Evaluate and adjust the information security program in light of the results of the required testing and monitoring; any material changes to the institution's operations or business arrangements; or any other circumstances that the institution knows or has reason to know may have a material impact on its information security program.

DESIGNATED EMPLOYEE

Designated Employee	Robert Kelley

RISK ASSESSMENT

Risk Assessment 2023

Includes:

- KEI Risk Assessment
- KEI Data Classification & Usage

- KEI Employee Confidentiality Policy
- KEI Student Information Security Policy

By: Kelley Education Inc.

About this Report

This report is on assessing risk to student information which is stored electronically & by physical means. The report was created & prepared by Robert Kelley who is IT responsible.

This is in Four Parts.

PART I RISK ASSESSMENT

STEP #1 INFORMATION COLLECTION

We collected information needed to assess risks.

- ✓ Interviewed employees
- ✓ Analyzed our systems & infrastructure
- ✓ Reviewed documentation

STEP #2 IDENTIFY & LOCATE VALUABLE ASSETS

Located all valuable assets across the organization that could be damaged by threats.

- ✓ Servers:
  - We employ an outside hosted server with an upgraded security oversight plan & backup data protection
  - We use GEMCOR, Inc. (see security plan)
  - We use a student information system by Orbund hosted on AWS
  - We use Lightheart, Sanders server to upload student files (security plan forthcoming from Lightheart, Sanders)
- ✓ Student Information System by Orbund LLC
  - Orbund is Soc 2 Type II certified
  - Resides on an SaaS platform
- ✓ Website
  - We use an outside firm to host our website to keep it separate from the server we use to hold certain student files.
  - We pay an outside service vendor to perform security monitoring, malware removal, & data restoration in the event of an attack
- ✓ Student files
  - Student files are those files located at each school & on the SIS.
  - Personally Identifiable Information is located in the students' financial aid files. When kept on campus, these files are located in a lockable office.

STEP #3 IDENTIFY POTENTIAL CONSEQUENCES

We identified 3 potential consequences.

- ✓ Legal consequences
- ✓ Data loss
- ✓ System of application downtime

STEP #4 IDENTIFY THREATS & THREAT LEVEL

We identified threats & the level associated with each.

Threat	Threat Detail	Threat Level
Natural Disasters	Flooding; Fire;	Low
System failure(s)	Electrical;	Low
Accidental human interference	Accidental	Low due to new safeguards on the SIS
Malicious human interference	Interference: damage by deleting data, a distributed denial of service (DDOS) against our website	Low
	Interception: hacking; data stolen	Low
	Impersonation: misuse of another's credentials	Low

STEP #5 ANALYZE CONTROLS

We analyzed controls that are either in place or in the planning stage to minimize or eliminate the probability that a threat will exploit a vulnerability.

Control Type	Description	Analysis
Technical Controls	Technical means; such as, but not limited to encryption, intrusion detection, authentication subsystems	We use 14-digit passwords for access to users; server access is limited to specific employees; software (file) access is limited to specific employees & controls are used within each software.
Non-Technical Controls	Non-Technical means security policies, administrative actions, training, & environmental & physical mechanisms.	We found weaknesses in our security policies & in our training.

STEP #6 IDENTIFY VULNERABILITIES & PROBABILITIES

Identified vulnerabilities & assess the likelihood of their exploitation.

Vulnerability		
Age of equipment	All equipment is recent; we found computers are destroyed after about 3-years & replaced; all pcs have user names & passwords	Not likely
Software design	Software is leased by outside vendors & updated regularly	Not likely
Software configuration	Software is leased by outside vendors & updated regularly	Not likely
Testing	We did not employ an outside firm to test individual pcs	Not likely

STEP #7 ASSESS THE IMPACT OF A THREAT

We assessed the impact that a threat could have & considered the following factors.

Factors	**Threat Impact**
mission of our systems & our processes	Low. Our mission would not be compromised. School records are redundant with backups & in some cases hard copies.
criticality of our systems determined by the value & the value of the data	Low. The criticality is not high as we would be able to continue our operations while we worked with redundant copies.
sensitivity of our system & data	High. Our information contains PII which could put our students at-risk.

STEP #8 PRIORITIZE HIGH SECURITY RISKS

Prioritized the high information security risks.

Threat/Vulnerability	**Level of Risk**
Accidental Human Interference	High
Sensitivity of our system & data	High

STEP #9 RECOMMEND CONTROLS

Based upon the Risk Assessment Report, we determined that the highest risks are from Accidental Human Interference. Further, we concluded that establishing policies & providing additional training would help control the security risk exposure.

Additionally, Robert Kelley discussed with each employee the need for greater control & confidentiality. Robert Kelley issued a Powerpoint presentation to each employee. In 2021, Robert Kelley will hold classes at each campus to deliver an updated version of the Powerpoint & to have an informed discussion with all employees.

Threat Vulnerability	**Control**
Accidental Human Interference	New controls through the SIS
	Acceptable Use Policy
	Administrative Data Backup & Restoration Policy
	Confidentiality Policy
	Email Systems & Usage Policy
Sensitivity of our system & data	Records Retention & Destruction Policy
	Identity Theft Red Flag Prevention
	Data Classification & Usage Policy
	PCI Policy (Through Intuit)

STEP #10 DOCUMENT

To support this report, we have completed the control recommendations & will review this information annually.

KEI DATA CLASSIFICATION & USAGE POLICY PURPOSE

The purpose of this policy to classify types of information & usage according to levels of confidentiality.

APPLICABILITY

This Policy applies to all employees, vendors, 3rd Party Servicers & those to whom confidential information has been entrusted by Kelley Education Inc. ("KEI").

DATA CLASSIFICATION

In information security, we classify data according to its level of confidentiality if it security is breached. In doing so, KEI hopes to determine security processes & controls to safeguard confidential information. KEI has organized data into 4 classifications.

1. Restricted Use
2. Confidential
3. Internal Use Only

4. Unrestricted

PART II DATA CLASSIFICATIONS DEFINITIONS & USAGE

RESTRICTED USE DATA - DEFINED

Restricted Use Data is data including Personally Identifiable Information (information which could identify an individual); financial information, health related information, & biometric data. Restricted Use Data requires the highest level of security. Examples include, but are not limited to:

- Social Security Numbers
- Tax Returns
- Driver License Numbers
- Financial Account Numbers

RESTRICTED USE DATA – USAGE RULES

1. Safeguarding - Restricted Use Data will always be safeguarded.
2. Digital Storage - Digital Restricted Use Data will be stored in institutionally supported applications residing in contracted server service except for data required for critical business purposes in an approved 3rd Party application.
3. Digital Access - Access to electronic data shall only be through an authenticated process & only by those granted access.
4. Hard Copy Storage - Hard copies shall be stored in locked rooms.
5. Hard Copy Access – Hard copy access is by authorized access only.
6. Additional Copies – Additional storage or copying (either electronic or hard copy) is not allowed except as required for compliance purposes.
7. Transmission – Transmission must be encrypted or via secure transmission.
8. When stored in the cloud, Restricted Use data will require multi-factor authentication.
9. Electronic and hard copy data shall be destroyed in accordance with Kelley Education Inc.'s Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form.

CONFIDENTIAL

This includes data protected by state or federal law, contractual agreements and proprietary information against unauthorized use, disclosure, modification and destruction. Confidential data includes the following:

1. Student records, including date of birth, place of birth, mother's maiden name, official grades recorded on a student's permanent record, academic information, race, judicial information and other information relative to a student's permanent record (i.e. official grades, judicial records, etc.).

2. Human Resources data including employment records, salary, benefits, personnel evaluations, date of birth, place of birth, mother's maiden name, race and other records pertaining to personnel files (i.e. payroll reports, yearly merit increase data, etc.).

3. Corporate records including Board of Trustee minutes, Board of Trustee votes and other confidential information dispersed at Board meetings and/or shared with Board members.

4. Sensitive Personal Information including credit checks, criminal background checks, visa numbers, sexual behaviors and criminal convictions (i.e. CORI/SORI reports).

5. Information security data, including administrator passwords used by Information Technology staff and other data associated with security-related incidents.

RULES FOR USAGE OF CONFIDENTIAL DATA

Confidential data shall be stored in institutionally supported applications located in Kelley Education Inc.'s contracted Cloud services; including those hosted by 3rd Party Servicers, institutionally supported shared drives, or approved third party hosted applications. Confidential data can be stored on Institute-owned laptop or desktop computers, but **shall not be** copied to non-Kelley Education Inc. computers, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

To this end, employees are permitted to store data on institutionally-owned laptop or desktop computers and shared drives; however, the dissemination of this data shall be done securely. Data shall not be transferred via e-mail unless encrypted. If data is transmitted on a recurring basis to external vendors, it is preferable to send this data through secure transmissions such as secure FTP (SFTP).

Electronic data shall be destroyed in accordance with Kelley Education Inc.'s Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form. All departments shall have policies in place and periodically review electronic storage areas and their hard copy storage areas to ensure that data is being destroyed in a timely and effective manner.

INTERNAL USE ONLY

This includes information that requires protection from unauthorized use, disclosure, modification, or destruction, but is not subject to any of the items listed in the Restricted Use or Confidential definitions above. Internal Use Only data includes:

1. Student ID

2. Data related to Kelley Education Inc.'s operations, finances, legal matters, audits, or other activities that are not public in nature, but not classified as Restricted Use or Confidential.

3. Grade worksheets (i.e. Excel files used to track student grading prior to submitting to software).

4. Personal white page, business white page or professional employment information for students, or alumni. This includes name, business name, business address, home address, e-mail, cell phone numbers, business phone numbers, home phone numbers, occupations and titles, but not classified as Restricted Use or Confidential.

5. Personal white page information for faculty and staff. This includes home address, cell phone, home phone, home fax and personal e-mail, but not classified as Restricted Use or Confidential.

6. Personal characteristics such as gender, height, weight, marital status, nationality, personal interests, photographs and names of children and other demographic information that is not classified as Restricted Use or Confidential.

7. Internal Kelley Education Inc. files, the distribution of which is limited by intention of the author, owner,
or administrator, but not classified as Restricted Use or Confidential.

RULES FOR USAGE OF INTERNAL USE DATA

Internal Use data can be stored in institutionally supported applications located in a Kelley Education Inc. contracted Cloud service, institutionally supported shared drives, third party hosted applications and laptop or desktop computers (both Kelley Education Inc. issued and personally owned). This data can be copied to smartphones, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

Employees are permitted to transmit this data via unencrypted e-mail. Electronic data can be destroyed using traditional application delete functionality. Hard copy information can be destroyed in accordance with an employee's personal or departmental policy.

UNRESTRICTED

This includes data that can be disclosed to any individual or entity inside or outside of KEI. Security measures may or may not be needed to control the dissemination of this type of data. Unrestricted data includes:

1. Content and images on Kelley Education Inc.'s public web sites

2. Publicly released press statements

3. School catalogs

4. Business White Page information for faculty and staff, unless otherwise restricted. This includes name, title, department, office location, office phone and KEI e-mail.

5. Published financial statements

RULES FOR USAGE OF UNRESTRICTED DATA

All information, whether in paper or electronic form, can reside in the public domain and is available to all students, faculty and staff; but it is subject to Kelley Education Inc.'s Acceptable Usage Policy and federal copyright laws.

POLICY ENFORCEMENT

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in KEI's Confidentiality Agreement.

APPROVAL AND REVISIONS

Policy Category: Confidential Student Information

Policy Approved By: Approved by Robert Kelley, President.

Policy Reviewed Annually By: Robert Kelley

Last Modified: 01 October 2023

PART III EMPLOYEE CONFIDENTIALITY POLICY

EMPLOYEE CONFIDENTIALITY POLICY PURPOSE

In accordance with the trust placed in its employees by Kelley Education Inc., all employees are responsible for maintaining the confidentiality of sensitive data; including but not limited to personal confidential information about individuals who enrolled or work at its schools.

EMPLOYEES

For the purposes of this policy, Kelley Education employees include educators, administrative staff, student educators, contract or, if applicable, casual employees.

SCOPE

Kelley Education Inc. maintains a number of policies to protect information. In accordance with these policies, all employees must protect sensitive information by using information only for approved purposes, controlling its dissemination, and reducing to the extent reasonably possible the risk of its unauthorized use or disclosure.

Additionally, Kelley Education Inc. employees may have access to other kinds of sensitive information that is protected by Federal, state, or local laws and regulations.

DISCIPLINE

Kelley Education Inc. employees are required to comply with all applicable laws and regulations and College policies. The failure to comply with policies or applicable laws & regulations regarding the use and safeguarding of sensitive information, or to protect other sensitive information not specifically covered by such policies, laws, or regulations, may result in disciplinary action. Disciplinary action may include termination of employment or enrollment at Kelley Education Inc.

PART IV STUDENT INFORMATION SECURITY POLICY

STUDENT INFORMATION SECURITY POLICY PURPOSE

The purpose of the Student Information Security Policy is to provide a written understanding of the expectation of confidentiality & safeguarding of confidential student information.

Technology changes on a daily basis. It allows students, faculty and staff work faster & more efficiently. Safeguarding information is becoming increasing difficult.

To protect the information of students, faculty, staff, alumni & others, Kelley Education Inc. has developed policies and processes to help classify, find and secure information in compliance with state and federal regulations.

KEI COMMUNITY

The Kelley Education Inc. ("KEI") community are employees, vendors, & 3rd Party Servicers hired to perform essential operations & may be provided access to "confidential student information."

CONFIDENTIAL INFORMATION

Confidential Information is any information that is not publicly available.

5 PHASES OF PROTECTING DATA

1. Identification. We have created a policy to determine what information is confidential. Please see the Data Classification & Usage policy which organizes data into 4 categories.
2. Rules. To learn how to use & store data that is restricted use, please see the Data Classification & Usage Policy.
3. Reviewing Data Collection. Kelley Education Inc. is working on developing Data Privacy Assessments to ensure that sensitive information is being handles correctly.
4. Retention & Destruction. To protect data, Kelley Education Inc. has created a Retention & Destruction Policy.
5. Awareness & Training. To understand threats, we will be updating our in-house training to share best practices.

POLICY PRINCIPLES

1. All Confidential Student Information is the property of KEI
2. Confidential Student Information is to be used only by those who have been given access
3. Confidential Student Information is to be used only to perform assigned duties
4. Confidential Student Information is to be safeguarded against loss, theft, or negligent handling
5. Confidential Student Information may not be used for profit or gain
6. Confidential Student Information is not to be shared with anyone not authorized to receive or to view it
7. Confidential Student Information will not be disclosed except in matters related to its accrediting body, legal or judicial, or government department. In all such cases Confidential Information will not be disclosed without the approval of the President or Director of Schools.

ENFORCEMENT

Any person or company that violates this policy will be subject to disciplinary action which may include termination & other disciplinary action as allowed by law.

APPROVAL & REVISIONS

Approved by: Robert Kelley on 01 October 2023.

SAFEGUARDS IMPLEMENTED

EMPLOYEE CONFIDENTIALITY

PURPOSE

In accordance with the trust placed in its employees by Kelley Education Inc., all employees are responsible for maintaining the confidentiality of sensitive data; including but not limited to personal confidential information about individuals who enrolled or work at its schools.

EMPLOYEES

For the purposes of this policy, Kelley Education employees include educators, administrative staff, student educators, contract or, if applicable, casual employees.

SCOPE

Kelley Education Inc. maintains a number of policies to protect information. In accordance with these policies, all employees must protect sensitive information by using information only for approved purposes, controlling its dissemination, and reducing to the extent reasonably possible the risk of its unauthorized use or disclosure.

Additionally, Kelley Education Inc. employees may have access to other kinds of sensitive information that is protected by Federal, state, or local laws and regulations.

DISCIPLINE

Kelley Education Inc. employees are required to comply with all applicable laws and regulations and College policies. The failure to comply with policies or applicable laws & regulations regarding the use and safeguarding of sensitive information, or to protect other sensitive information not specifically covered by such policies, laws, or regulations, may result in disciplinary action. Disciplinary action may include termination of employment or enrollment at Kelley Education Inc.

STUDENT CONFIDENTIALITY

PURPOSE OF POLICY

The purpose of the Student Information Security Policy is to provide a written understanding of the expectation of confidentiality & safeguarding of confidential student information.

Technology changes on a daily basis. It allows students, faculty and staff work faster & more efficiently. Safeguarding information is becoming increasing difficult.

To protect the information of students, faculty, staff, alumni & others, Kelley Education Inc. has developed policies and processes to help classify, find and secure information in compliance with state and federal regulations.

KEI COMMUNITY

The Kelley Education Inc. ("KEI") community are employees, vendors, & 3rd Party Servicers hired to perform essential operations & may be provided access to "confidential student information."

CONFIDENTIAL INFORMATION

Confidential Information is any information that is not publicly available.

5 PHASES OF PROTECTING DATA

1. Identification. We have created a policy to determine what information is confidential. Please see the Data Classification & Usage policy which organizes data into 4 categories.
2. Rules. To learn how to use & store data that is restricted use, please see the Data Classification & Usage Policy.
3. Reviewing Data Collection. Kelley Education Inc. is working on developing Data Privacy Assessments to ensure that sensitive information is being handles correctly.
4. Retention & Destruction. To protect data, Kelley Education Inc. has created a Retention & Destruction Policy.
5. Awareness & Training. To understand threats, we will be updating our in-house training to share best practices.

POLICY PRINCIPLES

1. All Confidential Student Information is the property of KEI
2. Confidential Student Information is to be used only by those who have been given access
3. Confidential Student Information is to be used only to perform assigned duties
4. Confidential Student Information is to be safeguarded against loss, theft, or negligent handling
5. Confidential Student Information may not be used for profit or gain
6. Confidential Student Information is not to be shared with anyone not authorized to receive or to view it
7. Confidential Student Information will not be disclosed except in matters related to its accrediting body, legal or judicial, or government department. In all such cases Confidential Information will not be disclosed without the approval of the President or Director of Schools.

ENFORCEMENT

Any person or company that violates this policy will be subject to disciplinary action which may include termination & other disciplinary action as allowed by law.

APPROVAL & REVISIONS

Approved by: Robert Kelley on 01 October 2023

PURPOSE

The purpose of this policy to classify types of information & usage according to levels of confidentiality.

APPLICABILITY

This Policy applies to all employees, vendors, 3rd Party Servicers & those to whom confidential information has been entrusted by Kelley Education Inc. ("KEI").

DATA CLASSIFICATION USAGE POLICY

DATA CLASSIFICATION

In information security, we classify data according to its level of confidentiality if it security is breached. In doing so, KEI hopes to determine security processes & controls to safeguard confidential information. KEI has organized data into 4 classifications.

1. Restricted Use
2. Confidential
3. Internal Use Only
4. Unrestricted

DATA CLASSIFICATIONS DEFINITIONS & USAGE

RESTRICTED USE DATA - DEFINED

Restricted Use Data is data including Personally Identifiable Information (information which could identify an individual); financial information, health related information, & biometric data. Restricted Use Data requires the highest level of security. Examples include, but are not limited to:

- Social Security Numbers
- Tax Returns
- Driver License Numbers
- Financial Account Numbers

RESTRICTED USE DATA – USAGE RULES

1. Safeguarding - Restricted Use Data will always be safeguarded.
2. Digital Storage - Digital Restricted Use Data will be stored in institutionally supported applications residing in contracted server service except for data required for critical business purposes in an approved 3rd Party application.
3. Digital Access - Access to electronic data shall only be through an authenticated process & only by those granted access.

4. Hard Copy Storage - Hard copies shall be stored in locked rooms.
5. Hard Copy Access – Hard copy access is by authorized access only.
6. Additional Copies – Additional storage or copying (either electronic or hard copy) is not allowed except as required for compliance purposes.
7. Transmission – Transmission must be encrypted or via secure transmission.
8. When stored in the cloud, Restricted Use data will require multi-factor authentication.
9. Electronic and hard copy data shall be destroyed in accordance with Kelley Education Inc.'s Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form.

CONFIDENTIAL DATA

This includes data protected by state or federal law, contractual agreements and proprietary information against unauthorized use, disclosure, modification and destruction. Confidential data includes the following:

1. Student records, including date of birth, place of birth, mother's maiden name, official grades recorded on a student's permanent record, academic information, race, judicial information and other information relative to a student's permanent record (i.e. official grades, judicial records, etc.).
2. Human Resources data including employment records, salary, benefits, personnel evaluations, date of birth, place of birth, mother's maiden name, race and other records pertaining to personnel files (i.e. payroll reports, yearly merit increase data, etc.).
3. Corporate records including Board of Trustee minutes, Board of Trustee votes and other confidential information dispersed at Board meetings and/or shared with Board members.
4. Sensitive Personal Information including credit checks, criminal background checks, visa numbers, sexual behaviors and criminal convictions (i.e. CORI/SORI reports).
5. Information security data, including administrator passwords used by Information Technology staff and other data associated with security-related incidents.

RULES FOR USAGE OF CONFIDENTIAL DATA

Confidential data shall be stored in institutionally supported applications located in Kelley Education Inc.'s contracted Cloud services; including those hosted by 3rd Party Servicers, institutionally supported shared drives, or approved third party hosted applications. Confidential data can be stored on Institute-owned laptop or desktop computers, but shall not be copied to non-Kelley Education Inc. computers, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

To this end, employees are permitted to store data on institutionally-owned laptop or desktop computers and shared drives; however, the dissemination of this data shall be done securely. Data shall not be transferred via e-mail unless encrypted. If data is transmitted on a recurring basis to external vendors, it is preferable to send this data through secure transmissions such as secure FTP (SFTP).

Electronic data shall be destroyed in accordance with Kelley Education Inc.'s Data Retention and Destruction Policy, and shall be rendered unreadable in paper or electronic form. All departments shall have policies in place and periodically review electronic storage areas and their hard copy storage areas to ensure that data is being destroyed in a timely and effective manner.

INTERNAL USE DATA

This includes information that requires protection from unauthorized use, disclosure, modification, or destruction, but is not subject to any of the items listed in the Restricted Use or Confidential definitions above. Internal Use Only data includes:

1. Student ID
2. Data related to Kelley Education Inc.'s operations, finances, legal matters, audits, or other activities that are not public in nature, but not classified as Restricted Use or Confidential.
3. Grade worksheets (i.e. Excel files used to track student grading prior to submitting to software).
4. Personal white page, business white page or professional employment information for students, or alumni. This includes name, business name, business address, home address, e-mail, cell phone numbers, business phone numbers, home phone numbers, occupations and titles, but not classified as Restricted Use or Confidential.
5. Personal white page information for faculty and staff. This includes home address, cell phone, home phone, home fax and personal e-mail, but not classified as Restricted Use or Confidential.
6. Personal characteristics such as gender, height, weight, marital status, nationality, personal interests, photographs and names of children and other demographic information that is not classified as Restricted Use or Confidential.
7. Internal Kelley Education Inc. files, the distribution of which is limited by intention of the author, owner,
1. or administrator, but not classified as Restricted Use or Confidential.

RULES FOR USAGE OF INTERNAL USE DATA

Internal Use data can be stored in institutionally supported applications located in a Kelley Education Inc. contracted Cloud service, institutionally supported shared drives, third party hosted applications and laptop or desktop computers (both Kelley Education Inc. issued and personally owned). This data can be copied to smartphones, USB devices or other portable media. Hard copy data shall be maintained in as few receptacles and rooms as business dictates. Copies of this data shall not generally be made unless business requires it.

Employees are permitted to transmit this data via unencrypted e-mail. Electronic data can be destroyed using traditional application delete functionality. Hard copy information can be destroyed in accordance with an employee's personal or departmental policy.

UNRESTRICTED

This includes data that can be disclosed to any individual or entity inside or outside of WPI. Security measures may or may not be needed to control the dissemination of this type of data. Unrestricted data includes:

1. Content and images on Kelley Education Inc.'s public web sites

2. Publicly released press statements

3. School catalogs

4. Business White Page information for faculty and staff, unless otherwise restricted. This includes name, title, department, office location, office phone and WPI e-mail.

5. Published financial statements

RULES FOR USAGE OF UNRESTRICTED DATA

All information, whether in paper or electronic form, can reside in the public domain and is available to all students, faculty and staff; but is subject to Kelley Education Inc.'s Acceptable Usage Policy and federal copyright laws.

POLICY ENFORCEMENT

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in WPI's Confidentiality Agreement.

APPROVAL AND REVISIONS

Policy Category: Confidential Student Information

Policy Approved By: Approved by Robert Kelley, President.

Policy Reviewed Annually By: Robert Kelley

Last Modified: 01 October 2023

OVERSEE SERVICE PROVIDERS

01 October 2023

This Institution employs 3 service providers.

1. GEMCOR Inc.
2. Wright Institutional Student Services
3. Prestige

This Institution has been in contact with each service provide to discuss, at least annually, its safeguards. This Institution is satisfied with each.

EVALUATION

This Institution routinely evaluates its security. As a result, this Institution has contracted a 3rd party to test its safeguards beginning in the 4th Quarter, 2023.