FLOYD COUNTY BOARD OF EDUCATION
Danny Adkins, Superintendent
106 North Front Avenue
Prestonsburg, Kentucky 41653
Telephone (606) 886-2354 Fax (606) 886-4550
www.floyd.kyschools.us

Date: October 18, 2018

Consent Agenda Item (Action Item): Approve the Data Security Policy by Career Cruising to purchase and partner for ILPs for grades 6-8.

Applicable Statue or Regulation: BOE Policy 01.11 General Powers and Duties of the Board.

Fiscal/Budgetary Impact: ILP Purchase is through Gear Up Funding for grades 6-8 and will not impact the general fund.

Recommended Action: Approve as presented

Contact Person(s): Courtney DeRossett, CIO

CIO Superintendent

Career Cruising

Data Security Policy

1. PURPOSE

The purpose of this policy is to outline essential roles and responsibilities within Career Cruising for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests and to establish a comprehensive data security program in compliance with applicable law.

This policy is also designed to establish processes for ensuring the security and confidentiality of sensitive information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information.

2. SCOPE

a. This policy applies to all Career Cruising employees, management, contractors, student interns, and volunteers.
b. This policy describes Career Cruising's objectives and policies regarding the maintenance and privacy of sensitive information.

3. DEFINITIONS

Term: Data Security Officer
Definition: The Data Security Officer provides administrative support for the implementation, oversight, and coordination of security procedures and systems with respect to specific data resources in consultation with internal and industry experts.

Term: Users
Definition: Users encompass all student, advisor, administrator, and staff roles within the Career Cruising data domain.

Term: Security Breach
Definition: A Security Breach is any event that causes or is likely to cause confidential information to be accessed or used by an unauthorized person and shall include any incident in which Career Cruising is required to make a notification under applicable laws such as FERPA.

Term: Level 1 Security Threat
Definition: A level 1 security threat is a threat that presents an immediate possibility of a security breach. Upon a Level 1 assessment, security threats are acted upon immediately and both internal and external notifications are sent out as soon as the impact is realized.

4. RESPONSIBILITIES

a. Executives/Management
    1) Establish program objectives
    2) Approve privacy policy
    3) Provide training for work force
    4) Designate Data Security Officer

b. Data Security Officer
    1) Develops privacy policies and procedures
    2) Coordinates and implements policy through organization's departments
    3) Oversees training
    4) Receives and processes privacy complaints
    5) Processes individual rights requests
        a) Right to access/copy protected information
        b) Right to restrict use/disclosure
        c) Right to confidential communications
        d) Right to an accounting of disclosures
        e) Right to file a complaint
    6) Ensures retention of policies and procedures, complaints, and investigative materials to meet compliance requirements.

c. Employee responsibilities
    1) Understand and comply with organization's policies regarding user confidentiality and privacy

5. CAREER CRUISING DATA DOMAIN

Career Cruising's data domain encompasses the following:

a. All student, parent, and advisor data transmitted to Career Cruising from an SIS or related extract.
b. All student, parent, and advisor data transmitted from Career Cruising to an SIS or related client data store.
c. All communications and interactions with clients.
d. All data-at-rest including archives and backups.

6. ACCESS TO DATA

a. Career Cruising uses the principle of least privilege in that users or software systems are granted only the least amount of privilege necessary to complete the job. These privileges are reviewed and audited on a regular basis to ensure compliance is maintained at all times.

b. In the performance of their daily work, some Career Cruising staff may come into contact with student data. As such, all staff members are required, as a term of their employment, to agree to the following clause:

> *The performance of your duties may involve a need to access and review confidential student information, including data protected by various privacy laws. The protection of each student's confidentiality and privacy is a legal obligation of the Company. As such, you agree to maintain the confidentially of this information and data, and prevent any re-disclosure, subject to applicable law, both during and after your employment with the Company.*

c. School staff are given access to the Career Advisor Management System. Staff access and security settings are determined by the school primary contacts.

7. OWNERSHIP AND RETENTION OF DATA

1. All of the data and written material that is entered by a Portfolio End User while using the Service ("Portfolio Work"), and the copyright associated with Portfolio Work, is owned by such Portfolio End User. The Portfolio End User will grant to Service Provider a non-exclusive, non-terminable, royalty-free, world-wide license to Portfolio Work and the copyright therein so that Service Provider can fulfill its obligations in accordance with this Terms of Use Agreement. As such, Service Provider shall be able to store, have a

copy of, create other backup copies of, give Site Administrators access to and delete Portfolio Work.

2. We will destroy portfolio data at the written request of a student (end user).

3. We will destroy portfolio or advisor data at the written request of the district, or in accordance to district contracts in the event that Career Cruising's services are discontinued by that state, province, or district.

8. SAFEGUARDS FOR THE PROTECTION OF CLIENT INFORMATION

a. Administrative safeguards: Career Cruising employees conform to strict data access policies and procedures, including the use of the principle of least privilege. We routinely test our security infrastructure with penetration tests and review and assess Internet threats as they become known.

b. Physical safeguards: Career Cruising uses a server colocation that provides the benefits of Canada's security, political stability, and strict privacy laws that provide a safe haven from malicious attacks. The infrastructure includes environmental control (constant temperature and humidity maintenance, particulates filtration), fire suppression systems, redundant power sources and UPS backup, large capacity of multi-homed quality bandwidth, round the clock physical security (card entry, video monitoring of the facilities), and available monitoring and technical services such as central data storage, backups, firewall and more.

c. Technical safeguards: Career Cruising follows industry best practices for database and file server security in addition to proactive logging and auditing of data access. Additionally, Career Cruising uses aggressive firewall configurations, SSL/TLS, and industry strength AES-256 backup encryption to protect offsite backups.

9. CUSTOMER & EMPLOYEE CONCERNS

a. Customers or employees with a concern regarding data security or related policies are directed to speak with Career Cruising's Data Security Officer: datasecurityofficer@careercruising.com

b. All concerns will be reviewed and responded to within 2 business day of receipt and sooner if the security threat is considered a level 1 security threat.

c. All concerned parties will be further notified as soon as action has been taken against a potential security threat or concern.

10. BREACH OF SECURITY

The entity responsible for support of the system under attack is required to:

1. Report the attack to their management and to colocation partners.
2. Block or prevent escalation of the attack where possible.
3. Follow instructions from management & colocation partners during investigation and preservation of evidence.
4. Implement recommendations from colocation partners.
5. Repair any damage to the system.

10.1.1 INTERNAL NOTIFICATIONS

1. The Data Security Officer must report all breaches to senior management in a timely manner.

10.1.2 EXTERNAL NOTIFICATIONS

To determine if unencrypted private or highly sensitive information has been acquired, the following will be considered:

1. The type of information that was compromised (see our definitions of highly sensitive information below).
2. Physical possession (lost or stolen devices?).
3. Credible evidence that information was copied or removed.
4. Length of time between intrusion and detection.
5. Purpose of the intrusion.
6. Ability to contact affected individuals.
7. Applicable local, state, or federal laws.

If it is determined that an external notification to the affected individuals is warranted, the following procedures will be followed:

1. Written notice shall be provided to the affected individuals using electronic mail.
2. If written notice to the affected individuals is not feasible, a direct phone call will be made in cases where we have a contact number.
3. Additionally, Career Cruising may issue an informational update to its web site issuing the details of the breach as well as contact information for concerned parties.

10.1.3 HIGHLY SENSITIVE INFORMATION

Examples of highly sensitive data that would warrant an external breach notification include (but are not limited to):

- Student ID, Name, Address, Phone, Date of Birth
- Records protected by FERPA or other student data privacy laws.
- Information subject to contractual confidentiality provisions.
- Passwords, salts, or personal security codes.