Security and FERPA Data

[Confidential/Redacted]

*All confidential/redacted information will be coded with [C/R]

Federal Education Release Privacy Act

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. FERPA applies to all schools that receive some form of funding from the U.S. Department of Education.

FERPA protects data from the student's educational record.

FERPA regulation generally means no one can release information on a student's record without first obtaining the student's permission.

Examples

FERPA does not protect certain directory information, though some schools have additional privacy policies protecting non-FERPA data.

FERPA Data Examples

Student User ID
Class Schedule
Student ID Number
Financial Aid Status
Course Grades

Directory Data (not protected by FERPA):

Student Email
Student Name
Enrollment Status
Academic Honors
Dates of Attendance

At [C/R], **our policy is to keep ALL personal data confidential.**

[C/R] and FERPA Compliance

As a third-party vendor, [C/R] is legally permitted to receive FERPA-protected data from client schools. Schools are not required to obtain student consent so long as certain conditions apply:

- [C/R] must perform services for which the institution would normally use employees.
- [C/R] must use the data ONLY as directed by the school.
- [C/R] must follow all non-disclosure guidelines described by FERPA. This means [C/R] employees may not re-disclose any personally identifiable information obtained from the school.

As a [C/R] *employee, you are expected to know and understand that you must take precautions to prevent the unauthorized release of data from students' educational records.*

[C/R] and FERPA Compliance

Do:

- Shred all printed FERPA data immediately after use.
- Discuss sensitive student data *only* with school-appointed administrators.

Do NOT:

- Give information about students over the phone to anyone except the [C/R].
- Transmit any sensitive student data via email or fax.
- Leave printed FERPA data on your desk, or in any easily accessible location.

Infrastructure and Access

- [C/R] uses a development site called Victory. All data on the development site is real customer data that has been scrambled so as to preserve confidentiality of FERPA and non-FERPA data.
- IT and Customer Support staff are given access to [C/R] systems as needed. This includes access to [C/R] .
- Sales staff do not generally require access our live system. If you are a sales representative and you believe you need to access the live system, please see Customer Support. Chances are that you can achieve your goal without access to the live system.

System Access

- Only two individuals have access to the server room:

  [C/R]
- [C/R] employees not permitted to install software on [C/R] PC's. All requests for software installation should be directed to [C/R] .
- Use of [C/R] systems is restricted and employees should consider all activity to be monitored. Most web access is blocked, with exceptions for .edu and .gov sites, as well as [C/R] sites.

Security

[C/R] Employee Password Security Policies:

- Never write passwords down.
- Do not share passwords with anyone.
- Construct complex passwords for all hardware and software used, and change them regularly.

Password Complexity Requirements for Customers:

- Administrators: Require at least one letter, number and special character.
- [C/R] : Require at least one letter and number.
- [C/R] No requirements besides those dictated by [C/R] .

Any violation of these security policies constitutes grounds for dismissal.

Verification of [C/R]

If a caller requests an administrator password over the phone, you must:

1. Verify the identity of the caller by phoning them at [C/R] number that [C/R] has on file.
2. Email password [C/R] on file.

Building Security

For physical security, [C/R] general premises are secured with steel doors, security cameras and reinforced windows. Points of entry to the building are secured by both a biometric lock and an alarm. [C/R] employees must follow the below guidelines to preserve the security of the premises.

Do not:

- Prop the front door in any way that will allow entry without use of the biometric lock.
- Leave visitors unattended while they are in the building.
- Park in any way that blocks building entryways or exits.

Do:

- Keep the front door locked at all times.
- Ask to see ID/badges for visitors.
- Escort visitors at all time during their visits.
- Have visitors sit up front while they are waiting for someone.

Security

Staff Responsibilities and Accountability

Effective information security requires staff involvement as it relates to their jobs. Staff is accountable for their actions and therefore they own any events occurring under their user identification code(s). It is staff's responsibility to abide by policies and procedures of all networks and systems with which they communicate.

Staff responsibilities include but are not limited to:

- **Access and release only the data for which you have authorized privileges and a need to know (including misdirected e-mail)**
- **Report information security violations to the Information Security Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of state owned information technology resources**
-

- **Abide by and be aware of all policies and laws (local, state, federal, and international) applicable to computer system use**
- **Protect assigned user IDs, passwords, and other access keys from disclosure**
- **Attend periodic information security training provided by [C/R] IT Security Branch**