FERPA & Student Data

Ellevation is subject to the Family Educational Rights and Privacy Act (FERPA) as operating under the "school official" exception, wherein student directory and PII (Personal Identifying Information) may be provided to third parties (such as Ellevation) if the third party:

- Performs an institutional service or function for which the school or district would otherwise use its own employees;
- Has been determined to meet the criteria set forth in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the educational records;
- Is under the direct control of the school or district with regard to the use of maintenance of education records; and
- Uses education records only for authorized purposes and may not re-disclose PII from educational records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).

As such, the following best practices regarding the handling of student data are required of all employees:

- Employ the rule of minimum access/data necessary to complete the responsibilities of your role;
- Never transmit PII via unencrypted means (plain email, unencrypted USB drives, unsecured websites, FTP);
- Never release student data to unauthorized parties;
- Use only approved, secure systems and tools to access, send, receive or manipulate student data;
- Destroy student data files (physical and electronic) immediately once they are no longer needed;
- Attend and complete all company information security and FERPA-related training.

Communication Systems

The use of all Ellevation electronic devices and network systems, including phones and voicemail, computers, the internet and email; company issued handheld communication devices, mobile or cell phones and faxing systems, are intended for Ellevation business use only and are Ellevation property. Employees' use of these devices and systems for personal reasons must be kept to a minimum, and must not violate any laws or company policies. Electronic communication to an external party is not allowed on any Ellevation computer or network except for company business purposes or during an approved break periods. All information transmitted, received, or stored using Ellevation networks and systems is the property of Ellevation and must be treated as confidential. Employees are not permitted to access, copy, store, or read any information from these systems without authorization. Electronic communications may not be forwarded outside or to any non-Ellevation email address(es).

Monitoring and No Expectation of Privacy

Ellevation team management reserves the right to monitor its systems and the content, including all emails and internet sites visited, to the extent permitted under applicable state and federal law. Ellevation may conduct such monitoring without notice and reserves the right to review such information at any time. Any information transmitted through or stored in Ellevation's computer or electronic systems should not be considered to be private. Even information deleted from Ellevation's systems can still be retrieved or recovered. No employee should expect that any use of Ellevation's systems is private. We reserve the right to monitor, access, and read any information stored on Ellevation's systems, with or without notice, and whether or not such materials may be password protected. We will review Internet activity and analyze usage patterns, and we may choose to act accordingly to insure that Ellevation's resources are devoted to maintaining the highest levels of productivity. As such, you should not use Ellevation systems for anything you would not want the company to know about. All email, data, files, or other electronic records on the Ellevation systems are subject to review by the company. All documents and electronic files on the Ellevation systems are the property of Ellevation and not of the employee.

Confidential Information

Documents with sensitive, proprietary, or confidential information should be protected by a password. In addition, employees will only allow Ellevation's assigned information technology employee, team manager, the Company's CEO, or People Operations employees to access the password to confidential documents. Employees may not add encryption keys to the systems without express authorization from their manager or Information Security Director.

Employees are prohibited to access pornography or other offensive sites; gambling sites; illicit "dark web" sites; steal or review others' confidential computer files; or attempt to damage Ellevation systems or computers. Ellevation reserves the right to restrict access to certain sites either through content filtering or written notice.

Prohibited Uses

Ellevation employees cannot post anything online that circumvents policies prohibiting unlawful discrimination against current employees or Ellevation applicants. Transmitting, retrieving, or storing communications or materials of a harassing nature, that contain derogatory or inflammatory remarks about an individual's race, sexual orientation, age, disability, religion, national origin, or physical attributes shall be transmitted. No abusive, profane, or offensive language, nor any violent, sexually explicit, or obscene materials are to be transmitted through Ellevation's electronic systems. Ellevation's systems may not be used for any other purpose which is disruptive, illegal, or against Ellevation's policy or contrary to its best interests. Solicitation of non-Ellevation business or any use of Ellevation's systems for personal gain is prohibited, unless authorized by Ellevation. Employees may have reasonable access to social media sites for business activity and/or personal activities at the office over the company's

systems. Ellevation authorizes occasional use so long as it does not interfere with the employee's work activities or productivity.

Violations

Employees should immediately notify their supervisor or manager of any violations of this policy. Any employee who violates this policy or otherwise abuses the privilege of Ellevation's systems will be subject to corrective action up to and including termination. If necessary, Ellevation also reserves the right to advise appropriate legal officials of any violations of the law.

Social Media Communications

Additionally, employees are personally responsible for anything they communicate on social media. If an employee discloses that they work for Ellevation, unless specifically authorized, the employee must add a disclaimer that views do not represent those of Ellevation. Any employee who violates this policy may be subject to discipline or possible termination with Ellevation.

Network Security

Computer software that is installed on Ellevation systems may not be downloaded, copied, reproduced, altered or used by a employee without prior authorization, unless it is legal and necessary to perform a employee's job responsibilities. Any violation of copyright laws may result in discharge from the company. Ellevation will cooperate with software vendors and government officials in prosecuting cases of copyright violation. Use of any "pirated" or "bootleg" software is not allowed on Ellevation systems. The use of personal data or software also is not allowed on Ellevation systems without prior authorization.

To avoid creating a network security risk, employees are not allowed to use their personal computers/laptops, tablets, email, phones, printers or any other technology device in connection with any Ellevation system or computer without prior authorization. Ellevation also will not be responsible for any lost, stolen or damaged personal property, including electronic property.

Failure to follow this policy may result disciplinary action up to and including termination. All Systems must be kept in working order and any repair and cleaning of computer systems due to negligence may be charged to the employee.

Personal Smartphone Policy (aka Bring Your Own Device - BYOD)

We know employees want easy access to connect to email and other work systems and tend to use their own mobile smartphone to do so. If you would like to elect to use your own mobile smartphone to access Ellevation email or other systems, please refer to Ellevation's "Smartphone Information Security Policy & Liability Waiver". Conducting company business or accessing company data from your personal device without the appropriate approval, compliance software install & configured, and liability waiver on file is expressly forbidden.

Social Media

Ellevation respects the right of any employee to maintain a blog or web page or to participate in a social networking, Twitter or similar site, including but not limited to Facebook and LinkedIn. However, to protect Company interests and ensure employees focus on their job duties, employees must adhere to the following rules:

All rules regarding confidential and proprietary business information apply in full to blogs, web pages, social networking, Twitter and similar sites. Any information that cannot be disclosed through a conversation, a note or an e-mail also cannot be disclosed in a blog, web page, social networking, Twitter or similar site.

Whether an employee is posting something on their own blog, web page, social networking, Twitter or similar site or on someone else's, if the employee mentions the Company and also expresses either a political opinion or an opinion regarding the Company's actions, the poster must include a disclaimer. The poster should specifically state that the opinion expressed is their personal opinion and not the Company's position. This is necessary to preserve the Company's goodwill in the marketplace.

Any conduct that is impermissible under the law if expressed in any other form or forum is impermissible if expressed through a blog, web page, social networking, Twitter or similar site. For example, posted material that is discriminatory, obscene, defamatory, libelous or threatening is forbidden. Company policies apply equally to employee social media usage.

Ellevation encourages all employees to keep in mind the speed and manner in which information posted on a blog, web page, and/or social networking site is received and often misunderstood by readers. Employees must use their best judgment when using these forms of media. Employees with any questions should review the guidelines above and/or consult with their manager. Failure to follow these guidelines may result in discipline, up to and including termination.

Employees should be careful to avoid unintentional disclosure of proprietary or other confidential information before posting or disseminating photographs or videos taken within the office or at other company-sponsored events.
You must comply with requests by the company to remove postings containing proprietary company information and do so as soon as is practicable. This includes, but is not limited to, photographs, programming code snippets, sales information, business news, and partner contract information.

Gifts

Employees may not accept gifts or entertainment exceeding $500 in value, or any personal loans, from customers, suppliers, volunteers, competitors or potential competitors, without the

express approval of his or her manager or supervisor. Employees who are unsure as to whether a third party falls under these categories are encouraged to ask their supervisor or another member of management before accepting any such gift.

Background Checks

All job applicants and employees of the Company must submit to background checks as a condition of employment. For employees in sensitive, finance-related positions only, background checks will include a credit check report. Background checks, which will include credit checks, will be conducted upon hire. From time to time, employees assigned to a particular customer account may be required to comply with additional customer requirements with respect to background checks.

Refusal to consent to such background checks, or failure to satisfactorily pass such background checks, may result in the withdrawal of an offer of employment, the Company's inability to assign the employee to work on certain customer accounts, and/or be grounds for discipline, up to and including termination.

All background check records are considered confidential documents.