DATA PROTECTION POLICY

Purpose

The purpose of the Data Protection Policy is to establish an enterprise-wide approach to protect data, applications, networks, hardware, and computer systems ("Systems") of Perspectives Charter Schools ("Perspectives") from unauthorized access, transmission, alteration, or destruction.

Scope

This Policy applies to each of Perspectives' information systems managed by the Information Technology department or by a third party on behalf of Perspectives, and all Perspectives employees, or authorized third parties, requiring access to information systems, computer equipment, and data owned and/or operated on behalf of Perspectives.

Policy

This Policy applies to each of Perspectives' information systems managed by the Information Technology department or by a third party on behalf of Perspectives, and all Perspectives, or authorized third parties, requiring access to information systems, computer equipment, and data owned and/or operated on behalf of Perspectives.

The Director of IT and Data or designee will be responsible for the development and annual presentation of the Data Protection Policy for review by Senior Management. Recommended changes will be incorporated into a revised Data Protection Policy pending approval of any budget changes prompted by the revisions.

The Information Technology department of Perspectives will utilize system and network tools to monitor Data Protection Policy compliance as part of their day-to-day oversight and management of the Association's organization's technology infrastructure. Violations of the Data Protection Policy will be addressed pursuant to the progressive discipline policy in the Student and Employee Handbook. Violations should be addressed as soon as administratively possible, but no later than 24 hours after the recognition of a violation.

All students will be presented with an Acceptable Use Policy for Perspectives' Electronic Networks Acknowledgement form (Attached as Appendix) that reflects elements of the Data Protection Policy which that are applicable to students. The presentation of the Acceptable Use Policy for Perspectives' Electronic Networks Acknowledgement will occur as part of the new student orientation and periodic communication of policies to existing students.

Prior to gaining access to Perspectives' Systems, an Employee must sign the Employee Handbook Acknowledgement document which will be filed with Human Resources.

The Director of IT and Data or designee designate may solicit an independent annual assessment of the Data Protection Policy, including, but not limited to, external network connections, subject to budget approval by Senior Management.

Data Classification and Management

All data should be reviewed on a periodic basis and classified according to its use, value, sensitivity, and importance or criticality to Perspectives. The classification level then guides the selection of protective measures to secure the information.

Currently defined classifications are listed below:

Data Classifications

- **Restricted —** Restricted information is highly valuable, highly sensitive business information, for which the security or protection is dictated by regulatory, legal or contractual requirements. Restricted information should be limited to only authorized and business partners with a specific business need. Significant damage could occur if Restricted information were to become available to unauthorized individuals or entities either internal or external to Perspectives. Unauthorized disclosure could violate regulatory, legal, or contractual requirements, damage Perspectives' reputation, or pose a risk of identity theft. **State and Federal laws require that unauthorized access to certain Restricted information must be reported within specified timeframes to the appropriate agency or agencies. All reporting of this nature to external parties must be done by or in consultation with the Office of the General Counsel.**

- **Confidential —** Confidential information is valuable information that is owned by Perspectives or entrusted to it by others, which shall not be released to the general public. Disclosure of such information may have a negative impact on Perspectives' interests. Confidential information may be shared with authorized , contractors, and business partners who have a business need, and which must be subject to a Confidentiality or Non-Disclosure agreement in accordance with this Policy.

- **Public —** Information that has been approved for release to the general public and may be accessed by any individual internally and externally. Disclosure of such information would not cause harm to Perspectives.

- **Personally Identifiable Information—** Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, as defined by the statutes and laws of the states in which the potentially impacted individuals reside. Examples include, but are not limited to, an individual's full name or first initial and last name plus: Social Security number (SSN), driver's license or state identification number, date of birth, personal email address or username with password that provides access to an online account, financial account information, fingerprints, and medical and healthcare information.

- **Protected Health Information —**The Health Insurance Portability & Accountability Act (HIPAA), 45 CFR Part 160, defines Protected Health Information (PHI) as individually

identifiable health information that 1) identifies an individual; 2) is created or received by a health care provider, health plan, employer, or health care clearinghouse; 3) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and 4) is transmitted by electronic media or transmitted or maintained in any other form or medium.

For the avoidance of doubt, it is recommended that all data be considered ”Restricted” unless explicitly stated otherwise and as such would be subject to the following handling requirements:

Data that is classified as Restricted must be encrypted during transmission over insecure channels which includes, but is not limited to, email, FTP, or other information transmission protocols.

Backups of data must be handled with the same security precautions as the data itself.

When systems, laptops, work stations, external storage devices, or mobile devices are disposed of or repurposed, data residing on those devices must be irretrievably deleted or destroyed consistent with industry best practices for the security level of the data.

No Perspectives -owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

Data owners must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

Data custodians are responsible for creating data repositories and data transfer procedures which protect data in a manner appropriate to its classification.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

Personnel accessing restricted data via remote access technologies are prohibited from copying, moving, or storing high risk data onto local hard drives and/or removable electronic media unless explicitly authorized for a defined business need.

Acceptable Use Policy for Perspectives’ Electronic Networks

This Policy governs students’ use of Perspectives’ electronic networks (“Network”), which includes Perspectives’ computers, Perspectives’ local and/or wide area network, and access to the Internet through Perspectives’ computers or its local and/or wide area network. Use of the Perspectives electronic network also includes any use of computers outside Perspectives’ electronic network that are used to access Perspectives’ electronic network. Additionally, use of Perspectives’ electronic network shall include use devices used to access the Perspectives electronic network, including, but not limited to cellular or mobile phones, smart phones, and

text messaging devices. Any electronic communications or files created on, stored on, or sent to, from, or via the Network are the property of Perspectives. Consequently, students do not have any expectation of privacy with respect to such messages and files.

Students will be given access to the Network in order to work on class assignments. Because of the wide variety of valuable and less-than-valuable websites on the Internet, this section serves as an Acceptable Use Policy (AUP) for users of the Network. By using the Network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor, or other appropriate staff.

Unacceptable Uses of the Computer Network or Internet

These are examples of unacceptable uses of the computer network or internet inappropriate activity on the Network. This list, however, is not exhaustive. Perspectives Charter Schools reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the Perspectives students and , or (2) other activities, as determined by Perspectives as inappropriate.

- Using the Network in a manner that violates any provision of Perspectives' Discipline Code;
- Criminal activities that can be punished under law;
- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous email sites; spamming; spreading viruses;
- Causing harm to others or damage to their property, such as:
- Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
- Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
- Damaging computer equipment, files, data, or the network in any way, including intentionally accessing, transmitting, or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
- Using any Perspectives computer to pursue "hacking," internal or external, or attempting to access information protected by privacy laws; or
- Accessing, transmitting, or downloading large files, including "chain letters" or any type of "pyramid schemes."
- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
- Using another person's account password(s) or identifier(s);
- Interfering with other users' ability to access their account(s); or
- Disclosing anyone's password to others or allowing them to use another person's account(s).
- Using the Network for commercial purposes:
- Using the Internet for personal financial gain;
- Using the Internet for personal advertising, promotion, or financial gain; or

- Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities, such as solicitation for religious purposes, lobbying for personal political purposes.

Student internet safety
Students under the age of eighteen should only access Perspectives accounts outside of school if a parent or legal guardian supervises their usage at all times. The student's parent or guardian is responsible for monitoring the minor's use; Students should not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others; Students should not meet in person anyone they have met only on the Internet; and Students must abide by all laws, this Acceptable Use Policy and all Perspectives security policies.

Penalties for improper use
The use of a Perspectives account is a privilege, not a right, and misuse will result in the loss of Network privileges. Misuse may also lead to further disciplinary and/or legal action for students, including suspension, expulsion, or criminal prosecution by government authorities.

Student Record Information

Notice concerning student records

The Illinois School Student Records Act ("ISSRA"), the federal Family Educational Rights and Privacy Act ("FERPA"), and the regulations issued pursuant to these laws require that the Board of Directors of Perspectives Charter Schools ("Perspectives") adopt a Student Records Policy ("Policy"). The Board of Directors has adopted a Policy and implementing Procedures which are available upon request from the school office.

Perspectives maintains both a permanent and temporary record for each student. The permanent record consists of basic identifying information concerning the student, his or her parents' names and addresses, the student's gender and date/place of birth, academic transcript, attendance record, health record, unique student identifier, scores received on all State assessment tests administered in grades 9-12, and a record of release of this information. It may also contain a record of honors and awards received, information concerning participation in school sponsored activities and organizations.

The temporary record consists of all other records maintained by Perspectives concerning the student and by which the student may be individually identified. It must contain a record of release of information contained in the temporary record, scores received on the State assessment tests administered in the elementary grade levels (K-8), a completed home language survey form, information regarding serious disciplinary infractions (i.e., those involving

drugs, weapons, or bodily harm to another) that resulted in punishment or sanction of any kind, biometric information, information regarding an indicated report pursuant to the Abused and Neglected Child Reporting Act, 325 ILCS 5/8.6, health-related information, and accident reports.

A parent, or any person designated as a representative by a parent, has the right to inspect and copy the student's permanent and temporary records except as limited by the Policy or state or federal law. A student has the right to inspect or copy his or her permanent record. (All rights of the parent become the exclusive rights of the student upon the student's 18th birthday, graduation from secondary school, marriage, or entry into military service, whichever comes first.) In order to review the student's record, a parent must make a written request to Perspectives. The request will be granted within fifteen (15) school days after the date of receipt of the request. Perspectives may charge a fee [not to exceed $0.35 per page] for copies of the record. This fee will be waived when the parent is unable to pay.

Release of records
Perspectives may be required to release information contained in student records without parental notice or consent to the following individuals or in the following circumstances:

To a Perspectives or State Board of Education employee or official with a demonstrable educational or administrative interest in the student. A school official is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer or contractor outside of the school who performs an institutional service or function for with the school would otherwise use its own and who is under the direct control of the school with respect to the use and maintenance of personally identifiable information from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student or other volunteer assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility:

- to any person for the purpose of anonymous research, statistical reporting or planning;
- in an emergency situation, if necessary to people's health and safety;
- in connection with a student's application for or receipt of financial aid;
- during an audit or evaluation of federally-supported education programs;
- as allowed under the Serious Habitual Offender's Compensation Action Program;
- to a governmental agency for the investigation of a student's school attendance;
- if the information is directory information, as explained below, and the parent has not informed the District that such information is not to be released;
- to accrediting organizations in order to carry out their accrediting functions,
- to the Illinois Department of Healthcare and Family Services for purposes of school breakfast and lunch programs; or
- Pursuant to a court order where a parent of a student is named in the court order.

Perspectives may also be required to release student records without parental consent to the following individuals or in the following circumstances, as long as parents/guardians are first notified of their right to inspect, copy or challenge the contents of the records to be released:

- to the records custodian of a school to which the student is transferring;
- pursuant to a court order where a parent of a student is not named in the court order;
- to any person as specifically required by law; or
- Pursuant to a reciprocal reporting agreement, or to juvenile justice authorities when necessary to complete their official duties.

Any other release of information requires the prior written consent of the parent. The parent has the right to request a copy of any released records.

Perspectives prohibits the disclosure by school to any person against whom the District has received a certified copy of an order of protection the location or address of the petitioner for the order of protection or the identity of the schools in the District in which the petitioner's child or children are enrolled. Perspectives shall maintain the copy of any order of protection in the record of the child or children enrolled in the District whose parent is the petitioner of an order of protection. In addition, no person who is prohibited by an order of protection from inspecting or obtaining school records of a student pursuant to the Illinois Domestic Violence Act of 1986 shall have any right of access to, or inspection of, the school records of that student.

A parent has the right to request the removal from their child's academic transcript of one or more scores received on college entrance examinations by submitting this request in writing to their school's Official Records Custodian. Contact your school's Office Manager for details. In the written request, the parent must state the name of each college entrance examination that is the subject of the request and the dates of the scores that are to be removed.

A parent also has the right to challenge or seek amendment to any entry in the student's school record, except for (1) grades; (2) name and contact information of Perspectives Official Records Custodian; and (3) references to expulsions or out-of-school suspensions, if the challenge to expulsions or suspensions is made at the time the records are forwarded to another school to which the student is transferring. Parents may challenge or seek amendment to a student's school record by claiming that the record is inaccurate, irrelevant, improper, misleading, or violation of the student's privacy rights. Perspectives' Student Records policy, and its accompanying Administrative Procedures, provide for hearing and appeal procedures and an opportunity to include a statement in the record discussing or explaining any entry. To challenge a record or entry, the parent must contact the Official Records Custodian. Parents may obtain a copy of Perspectives' Student Records Policy by contacting their school Office Manager.

The Policy also provides timelines for the destruction of records. Parents will be notified of the destruction schedule of the student's records at the time of graduation, transfer, or permanent withdrawal from the District. Permanent records are kept for sixty (60) years after the student leaves the District. Temporary records are kept for the period of their usefulness to the school, but in no case less than five (5) years after the student leaves a Perspectives Charter School. Student temporary records are reviewed by the District every four (4) years or when a student

changes attendance centers. A parent has the right to copy any student record, or information contained in it, proposed to be destroyed or deleted.

The law allows school districts to designate certain information as "Directory Information," which consists of identifying information. Perspectives has designated the following as Directory Information: [Note: Perspectives may choose to designate all, some or none of the following as directory information] the student's name, address, gender, grade level, birth date and place, and his/her parents' names, mailing addresses, electronic addresses, and telephone numbers; academic awards, degrees and honors received; information relating to school-sponsored activities, organizations, and athletics; major field of study; and period of attendance in the school. Directory Information also includes photograph, videos, or digital images used for informational or news-related purposes of a student participating in school or school-sponsored activities, organizations, and athletics that have appeared in school publications. However, photographs highlighting individual faces and used for commercial purposes require prior, specific, dated, and written consent of the parent or student, as applicable. An image on a school security videotape recording is not Directory Information. Further, student social security numbers or student identification or unique student identifiers are not Directory Information.

[Perspectives does not release Directory Information] or [Perspectives will release Directory Information to the general public from time to time, including by way of a school directory to be issued _____, a student yearbook to be issued _____, unless a parent informs Perspectives within ten (10) days of this Notice that information concerning his or her child should not be released, or that the parent desires that some or all of this information not be designated as Directory Information. In addition, the District will release a student's name, address, and telephone listings to military recruiters and institutions of higher education upon their request unless you advise us to the contrary in writing.]

Finally, no person may condition the granting or withholding of any right, privilege or benefit or make as a condition of employment, credit or insurance the securing by any individual of any information from a student's temporary record which such individual may obtain through the exercise of any right secured under the ISSRA or regulations.

If you believe that Perspectives has violated or is violating this policy, you have the right to file a complaint with the United States Department of Education concerning the District's alleged violation of your rights.

Student Cell Phone and Electronic Device Policy

Perspectives Charter Schools values student learning and engagement and seeks all opportunities to ensure students grow academically and through A Disciplined Life®. To this end, we do not want students distracted from learning through being on phones for any purpose not directed by the teacher.

To accommodate the growing parental concerns about student safety while traveling to and from school, Perspectives Charter Schools will allow students to possess cell phones only in locked lockers, on school grounds, as long as the following rules are strictly adhered to:

The use of cell phones and other personal electronic devices (including, but not limited to tablets, digital cameras, laptops, headphones, smart watches, iPods, and pagers, or any other electronic device deemed not appropriate for school use) in the school building, during normal school hours (including outgoing calls, incoming calls, text messaging, camera use, data use, game-playing, or any other use), or when representing Perspectives Charter Schools, **is strictly prohibited**. This includes the classrooms, lunchroom, hallways, and bathrooms, field studies and internships, during assemblies and with guest speakers unless the school has specifically stated otherwise. Cell phones and personal electronic devices should be turned off and in a locked locker as long as the student is in the building or attending a school-level event.

If a student is found using a cell phone or personal electronic device between the aforementioned hours, teachers, disciplinarians, and/or school administrators will confiscate the cell phone or personal electronic device and lock it up in the school office for the remainder of the day. Continued abuse of this privilege will result in disciplinary action and privileges will be revoked.

Students serving detentions or in-school suspensions are prohibited from using a cell phone or personal electronic device while serving his or her detention or in-school suspension. Cell phones and personal electronic devices should be turned off and put in a locked locker during detention or turned into a dean or member of the administration during in-school suspension. If a student is found using a cell phone or electronic device while serving a detention or in-school suspension, teachers, disciplinarians and/or a school administrator will confiscate the cell phone or electronic device and the student may be subject to additional consequences or ADL interventions outlined in the chart found on page 51. . Students can retrieve cell phones and personal electronic devices after detention or in-school suspension. Continued abuse of this privilege will result in disciplinary action and privileges will be revoked.

Phone messages to students

To alleviate unnecessary interruption of classroom instruction, only messages that are of an emergency nature will be accepted and delivered to students. Parents/guardians should continue to call the school for any emergency situation, and Perspectives staff will contact your child. Do not try to contact them by cell phone during school hours as their cell phones will be locked in their lockers. Any evidence showing that a student is acting on or replying to phone calls or messages received during school hours is a violation of school policy and may result in disciplinary actions.

It is strongly recommended that students NOT bring any valuable, portable electronic devices to school including, but limited to: such as iPods, tablets, laptops, digital cameras, Apple Watches or handheld games. Perspectives is not responsible for the theft, loss of any personal property including, but not limited to: money, clothing, shoes or damage to cell phones or any other personal electronic devices brought into the school. School officials are not responsible for searching, reviewing camera footage, investigating, or interrupting class, to recover any lost or stolen personal property.

Consequences for students who violate the Cell Phone and Electronic Device Policy include:

- Consequences
- Detention
- Confiscation of electronic device

If the device is confiscated and turned over to the school's main office, students can retrieve the device from the school office at the end of the day.

The use of camera phones and digital cameras is strictly forbidden in private areas, such as locker rooms, washrooms, dressing areas, classrooms, and offices at any time. Such use may also be in violation of the criminal code.

Employee Personal Use of Perspectives' Computers, Electronic Communication Systems, and Other Equipment

General provisions

The postage meter, copy machines, fax machines, computer equipment, telephone, etc.are for business use only. They are not to be used for personal reasons unless permission is given by your supervisor and arrangements are made to reimburse Perspectives where appropriate. Personal mail is not to be processed through the postage meter.

All of our Electronic Communications Systems [including, but not limited to, computers (software and hardware), the Internet, e-mail, and voicemail], as well as all information transmitted, received, or stored in these systems are the property of Perspectives. The Electronic Communication Systems are provided for employee use solely for business purposes. Thus, Perspectives needs to be able to access and/or disclose any information in the Electronic Communication Systems, even those protected by your personal password, at any time, with or without notice to the employee. have no expectation of privacy in connection with the use of these systems, or the transmission, receipt, or storage of information in such systems. Therefore, should not use the Electronic Communication Systems to store or transmit any information that they do not want management and/or other to see, hear or read.

Nothing should be communicated through the Electronic Communication Systems that would be inappropriate to communicate in any other manner in the workplace. Specifically, the Electronic Communication Systems are not to be used in a way that may be disruptive, illegal or offensive to others. The use of derogatory, inappropriate, discriminatory and/or non-professional language, including but not limited to slander, obscenity, sexual harassment, etc. is prohibited. Similarly, there is to be no display or transmission of sexually explicit images, messages or cartoons. Moreover, Electronic Communication Systems may not be used to solicit for any other business, organization, cause, group, commercial venture or other non-business matter.

Most of our Electronic Communication Systems are password protected to limit access to certain information, to protect data from tampering, and to identify the user. are required to keep their passwords confidential, and to comply with all security procedures. The unauthorized use of a password, or the access to, or retrieval of, information transmitted or stored in the Electronic

Communication Systems, is strictly prohibited.

Perspectives purchases and licenses the use of various computer software for business purposes and does not own the copyright to the software or its related documentation. Therefore, unless authorized by the software developer, neither Perspectives nor any of its third party providers has the right to reproduce such software for use on more than one computer. may only use software on local area networks or on multiple machines according to the software license agreement. Perspectives prohibits the illegal duplication of software and its related documentation.

Special Rules Regarding Use of the internet
Perspectives has systems in place that are capable of monitoring and recording all usage of Perspectives' internet facilities, including e-mail sent outside Perspectives. Specifically, our security systems are capable of recording (for each user) each internet site visit, each chat, newsgroup or e-mail message, and each file transfer into, and out of, our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her internet usage. Our managers will periodically review internet activity and analyze usage patterns, and they may choose to publicize this data to ensure that Perspectives' internet resources are devoted to maintaining the highest levels of productivity.

No employee may use Perspectives internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user. In this regard, no employee may use Perspectives' internet facilities to propagate any virus, worm, Trojan horse or trapdoor program code.

Each employee using the internet facilities of Perspectives shall identify himself or herself honestly, accurately, and completely when participating in chats or newsgroups; or when setting up accounts on outside computer systems.

Only those who are authorized to speak to the media on behalf of Perspectives may claim to be speaking or writing in the name of Perspectives to any newsgroup or chat room. Where an individual participant claims to be communicating on behalf of Perspectives, the employee must refrain from any political advocacy and from the unauthorized endorsement or appearance of endorsement by Perspectives of any commercial product or service not sold or serviced by Perspectives, or its affiliates.

Perspectives retains the copyright to any material posted to any forum, newsgroup, and chat or internet page by any employee in the course of his or her duties.

Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential or proprietary information of Perspectives, **except that may discuss terms and conditions of employment regarding themselves or their fellow, such as, for example: wages and working conditions.** Use of Perspectives' internet facilities to commit infractions such as misuse of Perspectives' assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are prohibited by

general Perspectives' policy and will be sanctioned under the relevant provisions of this Handbook.

Employees may use the internet facilities for non-business research or browsing during mealtime or other breaks, or outside work hours, provided that all other usage policies are strictly upheld. However, with internet access may not use Perspectives' internet facilities to download entertainment software or games or to play games over the internet. Rather, with internet access may download only software for business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.

Blogging and Social Networking

We need to be mindful about the public nature of social media and how it may impact your professional life here at Perspectives. While many of us are engaged in social networking on some level, need to be careful with respect to the content of our communications. To the fullest extent authorized by law, Perspectives prohibits the posting of comments or materials (including photographs, videos or audio) that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, or violates our policy against sexual or other unlawful harassment. This includes, but is not limited to, prohibited material (as described above) regarding Perspectives, our administrative staff, teachers, students, or the parents of students. Such actions constitute legitimate grounds for dismissal. It is important to note that such actions are prohibited, whether done during work hours or outside of work. Additionally, participation in social networking activities that can be characterized as non-work related and carried out during a time that you are scheduled to be working, can certainly interfere with your work duties and/or responsibilities and can be cause for appropriate disciplinary action.

We understand that social networks can be an important means of communicating with friends and family. However, be aware that anything you post online may sometimes be accessible to others outside of your "circle."

In addition to the above, stop and consider the following guidelines before hitting "send" or "post":

- We strongly discourage from being online "friends" with subordinates or with any Perspectives students. who become aware through social media or otherwise of suspected abuse or neglect of a Perspectives student are expected to contact their supervisor and DCFS.
- Blogs and other forms of online discourse are individual interactions, not Perspectives communications. You are personally and legally responsible for your communications. When discussing Perspectives related matters, you must identify yourself and make it clear that you are speaking for yourself and not on behalf of Perspectives. Where appropriate, use a disclaimer such as: "The postings on this site are my own and don't necessarily represent Perspectives' positions, conclusions or opinions."

- Adhere to the “common sense” rule outlined above so as to avoiding harassing or other prohibited communications with peers, subordinates, and students.
- Do not discuss or divulge confidential Perspectives information, for example: personal information about students, parents or that has not been made public or copyrighted materials. You are to consult Human Resources or your manager if you have questions about the appropriateness of publishing or disclosing information, concepts or developments related to our business on your site.
- You may respectfully disagree with Perspectives’ actions, policies, etc. However, to the fullest extent authorized by law, Perspectives prohibits any attacks that are unlawfully defamatory, threatening, coercive, or violate Perspectives’ policies prohibiting sexual or other unlawful harassment. Students, parents of students or others connected to Perspectives shall also be treated professionally.
- If a member of the media contacts you about your blog or posts or requests Perspectives information of any kind, you are to contact the Human Resources department.

Generally, what you do on your own time is your business. However, activities in or outside of work that affect your job performance, the performance of others, or Perspectives’ business interests are a proper focus for scrutiny. In some cases, it may result in disciplinary actions.

Violations

Employees should notify their immediate supervisor or the Human Resources department upon learning of violation of these policies. Those who violate these policies will be subject to disciplinary action up to, and including, discharge.

MEDIA POLICY

Perspectives has become a significant and very high profile charter school organization. As a result, Perspectives’ employees are increasingly “in the line of fire” regarding controversial issues. Perspectives respects the strong feelings have regarding these issues, and values their input and opinions. However, to avoid any unintentional misunderstandings and to protect the image and reputation of Perspectives in the community, must always adhere to the following rules:

- Only the CEO is authorized to speak to the media on Perspectives’ behalf. The only exception to this rule is where an employee receives prior express authorization from the CEO or his/her designee. More specifically, who claim to be speaking on behalf of Perspectives are required to obtain approval from the CEO before granting an interview to a newspaper or other media or engaging in any other communication with the media. However, continue to have the same rights as all citizens to speak out on matters of public concern to the extent provided by law, as long as they do so without representing themselves as a spokesperson for Perspectives or otherwise implying that they are speaking on behalf of Perspectives.

- Employees must have the CEO's explicit approval before using Perspectives' name on any non-work related publication or allowing any other organization to use Perspectives' name as a means of promoting their own agenda. Perspectives' name is proprietary to the School, and must always be treated as such.

- Employees shall not have so-called "off the record" conversations with the media regarding Perspectives' business or its alleged positions on controversial issues.

- If any employee in good faith believes that Perspectives should be taking a strong public position on a particular issue, then he or she should feel free to speak with the CEO. The CEO will then discuss the matter with the Board of Directors, and appropriate members of the management to determine what, if any, appropriate position should be formulated. In all cases, the CEO will make every effort to promptly respond to any such request.

- However, nothing in this policy precludes from discussing terms and conditions of employment about themselves or their fellow employees, such as, for example, wages and working conditions, provided that they do not represent that they are speaking on behalf of Perspectives (unless authorized to do so).

Privacy of Protected Health Information (PHI)

In 1996, Congress enacted HIPAA, a law designed, in part, to protect the privacy and confidentiality of individual health information. This policy sets forth the procedures and rules that will allow Perspectives to establish and maintain the privacy and confidentiality of individually identifiable health information as required by HIPAA's Privacy Rule.

In this Policy, "Protected health information" means individually identifiable health information transmitted or maintained by electronic media or any other form or medium excluding individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act and employment records held by Perspectives in its role as employer.

Privacy rule obligations
Perspectives is a "hybrid entity" since only some of its business operations concern the provision of health care services or the sponsoring of an employee health care plan. The Privacy Rule requires that Perspectives, as a hybrid entity, take a number of actions intended to protect the privacy of PHI. These actions include:

Identifying and documenting those operations which relate to the provision of health care services and the sponsorship of a health care plan and those who work with PHI as part of their duties.

Ensuring that those who do work with PHI do not disclose such information in a prohibited manner to other who are not involved in operations covered by the HIPAA privacy provisions.

Maintaining records and compliance reports that allow for a determination as to whether Perspectives is complying with applicable provisions of the Privacy Rule.

Cooperating with complaint investigations and compliance reviews to determine whether Perspectives is complying with applicable provisions of the Privacy Rule.

Permitting access to all documents that are pertinent to determining Perspectives' compliance with applicable provisions of the Privacy Rule.

Perspectives will also comply with the Minimum Necessary Standard Rule, meaning that those who work with PHI must make reasonable efforts to limit the use or disclosure to the minimum necessary to accomplish the intended purpose of the use or disclosure. To ensure compliance with the minimum necessary standard rule, officials shall take the following steps:

- Identify those or classes of who need access to PHI in order to carry out their duties;
- Determine the category or categories of PHI which the identified need to access and the appropriate conditions for the access;
- Make reasonable efforts to limit access of the identified to the PHI they need to conduct their duties.

Individual privacy rights

Individuals have a right to notice regarding the uses and disclosures of PHI that Perspectives may make, an individual's privacy rights pertaining to PHI and Perspectives' duties regarding PHI.

Individuals have the right to request that Perspectives' restrict the uses and disclosures of their PHI. If Perspectives does agree to a requested restriction, then the restricted PHI may not be used or disclosed unless the individual who made the restriction request needs emergency treatment and the restricted information is needed to provide emergency treatment.

Individuals have the right to request that they receive communications of PHI by alternative means or at alternative locations and Perspectives shall accommodate any such reasonable request.

Individuals have the right to inspect and obtain a copy of their PHI for as long as such information is retained by Perspectives in a designated record set, except in situations set forth by the Privacy Rule at 45 CFR § 164. 524.

Individuals have the right to request that Perspectives amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

Individuals have the right to receive an accounting of any disclosures of their PHI that Perspectives or any of its business associates has made during the six years prior to the date when the request for accounting was made. Perspectives shall not be required to provide an accounting for disclosures of PHI made for any of the reasons set forth by the Privacy Rule at 45 CFR § 164.528.

Privacy of Personally Identifiable Information (PII)

Sensitive Information is any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the privacy to which individuals are entitled under the Privacy Act.

Protected PII and Non-Sensitive PII: The Department of Labor has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the “risk of harm” that could result from the release of the PII.

Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general educational credentials, gender or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII. To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth and mother’s maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

PII and sensitive data must be secured and protected at all times.

1) All parties must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.

2) All parties must ensure that PII used during the performance of their grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

3) All parties must acknowledge that all PII data obtained through their program activity shall be stored in an area that is physically safe from access by unauthorized persons at all times and be managed with appropriate information technology (IT) services and designated locations. Accessing, processing and storing of PII data on personally owned equipment at off-site locations (e.g. employee's home, and non-managed IT services such as Yahoo mail) is strictly prohibited.

4) All parties who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards within the Federal and state laws.

5) All parties who have access to PII are required to sign a disclosure acknowledging the confidential nature of the data and must comply with safe and secure management of the data. These disclosures must be kept on file with the program service contractor for monitoring review at the request of the LWDB.

6) All parties must acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data, as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.

7) Access to any PII through program activity must be restricted to only those of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

8) All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means.

9) To ensure that PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email or stored on CDs, DVDs, thumb drives, etc., must be encrypted.

10) All PII data must be retained to satisfy all required record retention requirements. Thereafter, all PII data must be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

11) All parties must use appropriate methods for destroying sensitive PII in paper files (i.e. shredding) and securely deleting sensitive electronic PII.

12) Parties should not leave records containing PII open and unattended. Store documents containing PII in locked cabinets when not in use.

13) All Parties should immediately report any breach or suspected breach of PII to the Crisis Management Team so that legally required disclosures can be made.

Violations

All parties should notify their immediate supervisor or the Human Resources department upon learning of violation of these policies. Those who violate these policies will be subject to disciplinary action up to, and including, discharge.

Acceptable Use Policy for Perspectives' Electronic Networks

This Policy governs students' use of Perspectives' electronic networks ("Network"), which includes Perspectives' computers, Perspectives' local and/or wide area network, and access to the Internet through Perspectives' computers or its local and/or wide area network. Use of the Perspectives electronic network also includes any use of computers outside Perspectives' electronic network that are used to access Perspectives' electronic network. Additionally, use of Perspectives' electronic network shall include use devices used to access the Perspectives electronic network, including, but not limited to cellular or mobile phones, smart phones, and text messaging devices. Any electronic communications or files created on, stored on, or sent to, from, or via the Network are the property of Perspectives. Consequently, students do not have any expectation of privacy with respect to such messages and files.

Students will be given access to the Network in order to work on class assignments. Because of the wide variety of valuable and less-than-valuable websites on the Internet, this section serves as an Acceptable Use Policy (AUP) for users of the Network. By using the Network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor, or other appropriate staff.

Unacceptable Uses of the Computer Network or Internet
These are examples of inappropriate activity on the Network. This list, however, is not exhaustive. Perspectives Charter Schools reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the Perspectives students and , or (2) other activities, as determined by Perspectives as inappropriate.

- Using the Network in a manner that violates any provision of Perspectives' Discipline Code;
- Criminal activities that can be punished under law;
- Selling or purchasing illegal items or substances;

- Obtaining and/or using anonymous email sites; spamming; spreading viruses;
- Causing harm to others or damage to their property, such as:
- Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
- Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
- Damaging computer equipment, files, data, or the network in any way, including intentionally accessing, transmitting, or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
- Using any Perspectives computer to pursue “hacking,” internal or external, or attempting to access information protected by privacy laws; or
- Accessing, transmitting, or downloading large files, including "chain letters" or any type of "pyramid schemes."
- Engaging in uses that jeopardize access or lead to unauthorized access into others’ accounts or other computer networks, such as:
- Using another person's account password(s) or identifier(s);
- Interfering with other users' ability to access their account(s); or
- Disclosing anyone’s password to others or allowing them to use another person's account(s).
- Using the Network for commercial purposes:
- Using the Internet for personal financial gain;
- Using the Internet for personal advertising, promotion, or financial gain; or
- Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities, such as solicitation for religious purposes, lobbying for personal political purposes.

Student Internet Safety

Students under the age of eighteen should only access Perspectives accounts outside of school if a parent or legal guardian supervises their usage at all times. The student’s parent or guardian is responsible for monitoring the minor’s use;

Students should not reveal on the Internet personal information about themselves or other persons. For example, students should not reveal their name, home address, telephone number, or display photographs of themselves or others;

Students should not meet in person anyone they have met only on the Internet; and

Students must abide by all laws, this Acceptable Use Policy and all Perspectives security policies.

Penalties for Improper Use

The use of a Perspectives account is a privilege, not a right, and misuse will result in the loss of Network privileges. Misuse may also lead to further disciplinary and/or legal action for students, including suspension, expulsion, or criminal prosecution by government authorities.

Print Name of Student Signature of Student Date

_____ _____ _____

Print Name of Parent Signature of Parent Date

_____ _____ _____

Print Name of Staff Signature of Staff Date

Student Campus:

- ❏ Perspectives Rodney D. Joslin
- ❏ Perspectives Math and Science Academy
- ❏ Perspectives Leadership Academy
- ❏ Perspectives High School of Technology
- ❏ Perspectives Middle Academy