THE PINNACLE CODE

The School Policy Manual for Pinnacle Canyon Academy
A Public K-12 Charter School
210 North 600 East, Price, Utah 84501
(435) 613-8102 ↔ (435) 613-8105 (fax)
http://www.pcaschool.com

This school policy manual will be updated regularly as needed and will be posted on the school's webpage: www.pcaschool.com

TABLE OF CONTENTS

REVIEWED August 2025

7 DATA AND TECHNOLOGY POLICIES

7.1 ACCESS TO RECORDS

Pinnacle will grant access to any documents, papers, or other records which are pertinent to the Federal award, to the Federal awarding agency Inspectors General, the Comptroller General of the United States, and the pass-through entry (i.e., the USBE) or their authorized representatives for them to make audits, examinations, excerpts, and transcripts. The right also includes timely and reasonable access to subrecipient's personnel for the purpose of interview and discussion related to such documents.
2 CFR 200.337

7.2 SIS SYSTEM/STUDENT COMPUTER USAGE

Pinnacle is committed to providing students and staff with access to technology and resources that provide the most effective educational experiences possible. Pinnacle firmly believes that the valuable information and interactions available through computer network communications is fundamental to these experiences and far outweigh the small percentage of materials that are not consistent with educational goals. As global communication tools become available, it is imperative that individual users understand the benefits and responsibilities of accessing a growing collection of resources. Although Pinnacle has taken precautions to restrict access to controversial materials, it is impossible on a global network to control all access.

The **Acceptable Use Policy** provides details regarding the appropriate and inappropriate use of Pinnacle's computers. The procedures do not attempt to articulate all required or proscribed behavior by users. Successful operation of the school computer network requires that all users conduct themselves in a responsible, decent,

ethical, and polite manner while using the school computers. Users are ultimately responsible for their actions in accessing and using Pinnacle computers and computer networks. Users of Pinnacle's computers are expected to review and understand the guidelines and procedures in this document. Before any student will be given access Pinnacle's computer resources, the student must present the "Acceptable Use Agreement" (AUA) form, properly signed by a parent or guardian, which AUA acknowledges that Pinnacle is not responsible for unauthorized or improper access or use of Pinnacle's Computer Network Communications services.

7.3 ACCEPTABLE USE POLICY

Pinnacle is committed to providing students and staff with access to technology and resources that provide the most effective educational experiences possible. Pinnacle firmly believes that the valuable information and interactions available through computer network communications is fundamental to these experiences and far outweigh the small percentage of materials that are not consistent with educational goals.

As global communication tools become available, it is imperative that individual users understand the benefits and responsibilities of accessing a growing collection of resources. Although Pinnacle has taken precautions to restrict access to controversial materials, it is impossible on a global network to control all access.

The Appropriate Use Policy that follows provides details regarding the appropriate and inappropriate use of Pinnacle's computers. The procedures do not attempt to articulate all required or proscribed behavior by users. Successful operation of the school computer network requires that all users conduct themselves in a responsible, decent, ethical, and polite manner while using the school computers. You, the user, are ultimately responsible for your actions in accessing and using District computers and the District computer network. As a user of Pinnacle's computers, you are expected to review and understand the guidelines and procedures in this document.

Before any employee or student will be given access Pinnacle's computer resources, the employee or student must present the "Acceptable Use Agreement" (AUA) form, properly signed by the employee or by the student and a parent or guardian, which AUA acknowledges that Pinnacle is not responsible for unauthorized or improper access or use of Pinnacle's Computer Network Communications services. To maximize the benefits of these tremendous resources, and to avoid abuse or access to inappropriate information and services, the Pinnacle Board of Education has adopted the following "Acceptable Use" policy.

Student Usage Guidelines

Responsibility: Access is a privilege, not a right. Access entails responsibility.

- The Board expects that staff will integrate thoughtful use of networked information resources throughout the curriculum.
- Student access from Pinnacle to telecommunications and networked information resources shall follow guidelines developed for the selection of appropriate instructional materials and shall be directed to resources evaluated prior to use.
- Since access could extend beyond evaluated or previewed resources, the staff will supervise and provide developmentally appropriate guidance and instruction to students in the appropriate and effective use of such resources.
- Students are responsible for appropriate behavior on school computer networks, just as in classrooms and other areas of the school corporation. Communications on networks are often public in nature.
- Outside of school, families are responsible for setting and conveying the same standards that their children exercise in the use of television, telephones, radio, movies and other media to the use of telecommunications and networked information resources. Therefore, Pinnacle supports and respects each family's decision whether or not to apply for student access and to request alternative activities not requiring access.

- The educational value of student networked information resources access is the joint responsibility of students, parents, and employees of the school corporation.
- Students will adhere to all UEN UtahLINK Network Acceptable Use Policy (see below).

Rights and Privileges: The network services are provided for educationally related communication, research and other activities. Access to Pinnacle network services will be provided to students who agree to act in a considerate and responsible manner.

- Students will submit a properly signed Acceptable Use Agreement, which includes staff and parental/guardian permission, to the network administrator.
- A network account, as well as an SIS account will include a username or number and private password, assuring that access is the responsibility of the student. In some cases, Pinnacle's system administrator may issue a limited "class" account to groups of students which may be used for specific purposes for a specific amount of time.
- Each student or "class" with network access shall be assigned storage space on the corresponding file servers that may be treated like school lockers.
- Network security is designed to allow access to these spaces only by the assigned user; however, network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Teachers may also review files for paperless grading of assignments.
- Users shall not expect that files stored on district resources will always be private.
- Parents are permitted to use school computers to check their own students' grades via the SIS system. Parents may also make arrangements to use school computers for school use activities. School computers are not to be used by parents for personal use.

Restrictions: The following activities are **not permitted** on Pinnacle's electronic resources
BOARD APPROVED: May 2025

- Accessing, uploading, downloading, transmitting, displaying, or distributing obscene or sexually explicit material; transmitting obscene, abusive, or sexually explicit language.
- Damaging computers, computer systems or computer networks; vandalizing, damaging or disabling the property of another person or organization; debilitating or disabling computers, systems or networks through the intentional misuse or overuse of electronic distribution or the spreading of computer "viruses" through the inappropriate use of files or diskettes.
- Engaging in practices that threaten the network (e.g., loading files that may introduce a virus).
- Harassing, insulting or attacking others.
- Violating copyright, or otherwise using another person's intellectual property without his or her prior approval or proper citation; using another person's passwords; trespassing in another person's folders, work or files.
- Using others' passwords.
- Trespassing in others' folders, documents, or files.
- Intentionally wasting limited resources.
- Employing the network for commercial purposes, financial gain, or fraud.
- Violating regulations prescribed by the network provider.
- Promoting, supporting or celebrating religion or religious institutions.
- Violating local, state or federal statute.
- Gambling of any kind including, but not limited to, online poker, online gaming, and sports betting.

Disclaimers: Pinnacle makes no warranties of any kind, either expressed or implied, for the access being provided.

- The staff, the school, and the Board of Education are not responsible for any damages incurred, including, but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on Pinnacle resources, or for personal property used to access Pinnacle resources.
- Pinnacle will not be responsible for the accuracy, nature, or quality of information stored on Pinnacle resources or gathered through school-provided access.

- Pinnacle will not be responsible for unauthorized financial obligations resulting from use of school-provided access.
- Further, even though Pinnacle may use technical or manual means to regulate access and information, these methods do not provide a foolproof means for enforcing the provisions of this policy.

Sanctions: Disciplinary action related to student access to electronic resources may be determined at the building and/or classroom level in accordance with existing practice regarding inappropriate language or behavior, as stated in the student code of Conduct.

- Violations of the school acceptable use policies may result in a loss of access to electronic resources, suspension, or expulsion.
- Additional sanctions for inappropriate behavior and communication shall be governed by the school discipline policy.
- When appropriate, law enforcement agencies may be involved.

Employee Usage Guidelines

Pinnacle expects everyone to exercise good judgment and use the computer equipment in a professional manner. Your use of the equipment shall relate to the school's goals of educating students and/or conducting Pinnacle business. Pinnacle recognizes, however, that some personal use is inevitable, and that incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with school business, and is not otherwise prohibited by Pinnacle policy or procedures.

Responsibilities, Rights and Privileges:

Use of School Software

School software is licensed to Pinnacle by a large number of vendors and may have specific license restrictions regarding copying or using a particular program. Users of this software must obtain permission from the IT Director prior to copying or loading Pinnacle software onto any computer, whether the computer is privately owned or is a school Computer.

Use of Non-Pinnacle Software

Prior to loading non-Pinnacle licensed software onto school computers (including laptops and desktops); a user must receive permission from the IT Director. All software must be legally licensed by the user prior to loading onto school equipment. The unauthorized use of and/or copying of software is illegal. It is against Pinnacle practice for staff or students to copy or reproduce any licensed software on Pinnacle computing equipment, except as expressly permitted by the specific software license. Unauthorized use of software is regarded as a serious matter and any such use is without the consent of Pinnacle and will be referred to the Board of Education for Disciplinary Action.

Privacy

District Computers, the Internet, and use of email are not inherently secure or private. For example, the content of an email message, including attachments, is most analogous to a letter or official memo rather than a telephone call, since a record of the contents of the email may be preserved by the sender, recipient, any parties to whom the email may be forwarded, or by the email system itself. It is important to remember that once an email message is sent, the sender has no control over where it may be forwarded and deleting a message from the user's computer system does not necessarily delete it from the school computer system. In some cases, emails have also been treated as public records in response to a public records disclosure request. Likewise, files, such as Internet "cookies" may be created and stored on a computer without the user's knowledge.

Users are urged to be caretakers of your own privacy and to not store sensitive or personal information on Pinnacle Computers. The school may need to access, monitor, or review electronic data stored on Pinnacle Computers, including email and Internet usage records. While Pinnacle respects the privacy of its staff; however, Pinnacle reserves the right to monitor or review electronic information for any reason. Pinnacle may monitor and review

the information in order to analyze the use of systems or compliance with policies, conduct audits, review performance or conduct, obtain information, or for other reasons.
Pinnacle reserves the right to disclose any electronic message to law enforcement officials, and under some circumstances, may be required to disclose information to law enforcement officials, the public, or other third parties, for example, in response to a document production request made in a lawsuit involving Pinnacle or by a third party against the user or pursuant to a public records disclosure request.

Care for Pinnacle Computers
Users of Pinnacle Computers are expected to respect the school's property and be responsible in using the equipment.

Users are to follow any instructions given regarding maintenance or care of the equipment. Users may be held responsible for any damage caused by your intentional or negligent acts in caring for school computers under your control. Pinnacle is responsible for any routine maintenance or standard repairs to school computers. Users are expected to timely notify the technology department of any need for service. Users are not to delete or add software to school computers without school permission. Due to different licensing terms for different software programs, it is not valid to assume that if it is permissible to copy one program, then it is permissible to copy others.

Using Email Wisely
Email encourages informal communication because it is easy to use. However, unlike a telephone call, email creates a permanent record that is archived and often transmitted to others. Remember that even when you delete an email from your mailbox; it still may exist in the system for some period of time. Be circumspect about what you send and to whom. Do not say anything in an email that you would not want to see republished in Internet email or hard copy. Remember that email invites sharing; a push of the button will resend your message worldwide, if any recipient (or hacker) decides to do so. What you say can be republished and stored by others. Beware of the "Reply All" button. Often your message only needs to be returned to one individual -- is the message really appropriate for (and shall it really take the time of) everyone on the address list.

You can create liability for yourself and the school. For example, within or outside the school, if you "publish" (type or resend) words that defame another individual or disparage another individual or institution, if you upload or download or resend copyrighted or pornographic material, if you use email to harass or discriminate against someone, or if you send private information or data about someone, you may violate applicable laws and Pinnacle policy. Make sure none of your activities violate any law or policy. Please keep in mind that because of intermediary server problems and other potential delays, Internet email can sometimes take anywhere from five minutes to several days to arrive. It may not be the best means to send time-sensitive information.

Using the Internet Access Wisely
Be circumspect about where you go and what you do. Do not visit any site or download or share any material that might cause anyone to question your professionalism, or Pinnacle's. Read the "License" or "Legal" contract terms on every site. Do not purport to bind the school to any license or other contract. If you make an agreement on your own behalf, do not violate that agreement using the school equipment or Internet account. Do not assume that just because something is on the Internet, you may copy it. As a general rule, assume that everything is copyrighted and do not copy it unless there is a notice on the site stating that you may do so. For example, if you see a clever cartoon assume that you may NOT copy it. Governmental documents are an exception (you may copy them), but you must confirm that it is the "government" and not a government-related entity such as the post office. Be aware of the "Do you want a cookie?" messages (if you have configured your browser to get such messages). If you answer yes, whatever activity in which you are engaged will be logged by the site owner to help it or its advertisers develop a profile about you or the school. It is possible that your browser is set to accept cookies without asking you each time. You can create liability for yourself and the school. For example, if you "publish" (type or re-send) words that defame or disparage another individual or institution, if you upload or download or re-send copyrighted or pornographic material, if you use the Internet to harass or discriminate against someone, or if you provide private information or data about someone, you may violate applicable laws or Pinnacle policy. Make sure none of

your activities violate any law or policy. Do not engage in any "spamming" or other activities that could clog or congest Internet networks.

Webpage/Online Learning Platforms (See Board Approved Change at EP 17. Teacher Webpages/Online Learning Platforms).
Teachers are required to create and maintain a webpage. If a teacher uses an online learning platform (Google classroom, Showbie or Canvas) that online platform fulfills this requirement. Your webpage/online learning platform may contain pictures of groups of students, student work, or student web pages. **You must verify that permission to post a student picture or work has been granted to the school by the student's parent or guardian.** Names shall not be posted with student pictures to protect the privacy of the students. Pictures of individual students shall only be posted as an exception, such as a contest winner with the specific permission of the parent or guardian.

UEN
Employees will adhere to the UEN UtahLINK Usage Policy below. Certified employees shall maintain a MYUEN account. MYUEN is a state supported resource for educational personnel.

SIS (Student Information System)
Teachers are required to record attendance and grades via the use of SIS. Teachers will be issued a user login and password. This password shall only be shared with the SIS administrator. Grades shall be posted in a timely manner, preferably weekly; however, grades are required to be posted every two weeks or according to the progress report schedule.

SSID (State Student Identification)
Employees who are given the responsibility and access to the SSID system must adhere to the policy set forth by USOE. USOE requires an adherence signature and background check on such employees.

Restrictions:
Pinnacle Computers may not be used for the following purposes:

- Commercial Use: Using School Computers for personal or private gain, personal business, or commercial advantage is prohibited.
- Political Use: Using School Computers for political purposes in violation of federal, state, or local law is prohibited. This prohibition includes using school computers to assist or to advocate, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office. The use of school computers for the expression of personal political opinions to elected officials is prohibited. Only those staff authorized by the CAO may express the District's position on pending legislation or other policy matters.
- Illegal or Indecent Use: Using School Computers for illegal, harassing, vandalizing, inappropriate, or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material), or in support of such activities is prohibited. Illegal activities are any violations of federal, state, or local laws (for example, copyright infringement, publishing defamatory information, or committing fraud). Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that (1) have the purpose or effect or creating and intimidating, a hostile or offensive environment; (2) have the purpose or effect of unreasonably interfering with an individual's work or school performance, or (3) interfere with school operations. Vandalism is any attempt to harm or destroy the operating system, application software, or data. Inappropriate use includes any violation of the purpose and goal of the network. Indecent activities include violations of generally accepted social standards for use of publicly-owned and operated equipment.
- Non-School Employee Use: District Computers may only be used by Pinnacle staff and students, and others expressly authorized by Pinnacle to use the equipment. Parents and Volunteers may only use school computers for the use of checking their student's grades and activities pertaining to the school as assigned by school personnel. Parents and other volunteers are not allowed access to the administrative side of the SIS or the SSID systems.

- Disruptive Use: Computers may not be used to interfere or disrupt other users, services, or equipment. For example, disruptions include distribution of unsolicited advertising (“Spam”), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of Pinnacle Computers or other resources accessible through the schools computer network ("Cracking" or "Hacking").

Sanctions
The Appropriate Use Policy is applicable to all users of Pinnacle Computers and refers to all information resources whether individually controlled, shared, stand alone, or networked. Disciplinary action, if any, for students, staff, and other users shall be consistent with the school’s standard policies and practices. Violations may constitute cause for revocation of access privileges, suspension of access to school computers, other school disciplinary action, and/or appropriate legal action. Specific disciplinary measures will be determined on a case-by-case basis.

Disclaimers
Pinnacle makes no warranties of any kind, either expressed or implied, for the access being provided. The staff, the school, and the Board of Education are not responsible for any damages incurred, including, but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on Pinnacle resources, or for personal property used to access Pinnacle resources. Pinnacle will not be responsible for the accuracy, nature, or quality of information stored on Pinnacle resources or gathered through school-provided access. Pinnacle will not be responsible for unauthorized financial obligations resulting from use of school-provided access. Further, even though Pinnacle may use technical or manual means to regulate access and information, these methods do not provide a foolproof means for enforcing the provisions of this policy.

Pinnacle provides a wide range of computer resources to its students and staff for the purpose of advancing the educational mission of the school. As a user of Pinnacle computers, you are expected to review and understand the Acceptable Use Policy and sign an Acceptable Use Agreement.

UTAH EDUCATION NETWORK ACCEPTABLE USE POLICY

Purpose of UtahLINK for Public Schools:
The purpose of the use by Utah Public Education of UtahLINK, the educational network supported by the Utah Education Network (UEN), is to advance and promote a world-class public education in Utah. UtahLINK is intended to assist in the collaboration and exchange of information between and among schools, school offices, the Utah Education Network, and other State and educational entities as well as provide access to the 'world of information' via networking facilities like the Internet.

UtahLINK's Goal for Public Schools:
The goal of UtahLINK is to promote innovation and educational excellence in Utah's public schools by facilitating resource sharing and expanded communications capabilities. To achieve this, the Network must provide quality, equitable, and cost-effective information and communication resources to the public education community.

UtahLINK's Mission Statements & Priority Listing for Public Education:
- To provide electronic mail service and electronic conferencing capabilities to public school professional employees;
- To provide basic services at no cost to public education end users;
- After first providing basic services, to provide opportunities for wider networking (interstate and international) by promoting the addition of full Internet services where economically feasible and deemed appropriate by the State Board of Education and UEN;
- To provide for both administrative and instructional file transfer capabilities where feasible.

UtahLINK Use by the Public Schools:
All use of UtahLINK shall be consistent with the purpose, goal, and mission of the Network. Successful operation of the network requires that its users regard UtahLINK as a shared resource, and cooperate to form a community of

diverse interests in an effort to promote educational excellence and provide world-class education throughout the state of Utah. It is therefore imperative that UtahLINK members conduct themselves in a responsible, decent, ethical, and polite manner while using the network. Further, they must abide by all local, state and federal laws. To ensure the smooth and continued operation of this valuable resource, members must accept the responsibility of adhering to high standards of professional conduct and strict guidelines.

The intent of the UtahLINK Public Education Acceptable Use Policy is to ensure that all uses of UtahLINK are consistent with its stated purpose, goal, and mission. UtahLINK is an open network in both implementation and spirit and encourages the pursuit of higher knowledge. However, it is important to recognize that with increased access to computers and people all over the world also comes the availability of controversial material that may not be considered of educational value in the context of the school setting. Further, UtahLINK recognizes the importance of each individual's judgment regarding appropriate conduct in maintaining a quality resource system. And while this policy does not attempt to articulate all required or proscribed behavior by its members, it does seek to assist in such judgment by providing the following guidelines:

I. Any use of UtahLINK for illegal or inappropriate purposes or to access materials that are objectionable in a public school environment, or in support of such activities, is prohibited. Language that is deemed to be vulgar is also prohibited. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Inappropriate use shall be defined as a violation of the intended use of the network, and/or purpose and goal. Objectionable is defined as materials that are identified as such by the rules and policies of the Utah State Board of Education that relate to curriculum materials and textbook adoption.

II. All use of UtahLINK must be in support of a world class public education and educational research in Utah and consistent with the purposes of the network;

III. The following uses are also prohibited: any use for commercial purposes or financial gain, any use for product advertisement or political lobbying, and/or any use which shall serve to disrupt the use of the network by other users.

IV. UtahLINK accounts shall be used only by the authorized owner of the account. Account owners are ultimately responsible for all activity under their account;

V. Unbridled and open-ended use of the network in terms of access time cannot be accommodated due to cost. Users are cautioned to exercise prudence in the shared use of this resource;

VI. All communications and information accessible via UtahLINK shall be assumed to be private property. Great care is taken by the UtahLINK's administrators to ensure the right of privacy of users. However, it is recommended that users not give out personal information like home addresses and/or telephone numbers. Also, passwords shall be kept private and changed frequently;

VII. Neither the USOE nor the UEN have control of the information on the Internet. Other sites accessible via the Internet may contain material that is illegal, defamatory, and inaccurate or potentially offensive to some people;

VIII. Under prescribed circumstances; public school student use may be permitted, provided proper supervision is maintained by school officials and parents;

IX. Under prescribed circumstances*, non-educator use may be permitted, provided such individuals provide evidence that their use furthers the purpose and goal of the network and public education in general;

X. As necessary, the Utah State Office of Education will determine whether specific Public Education uses of UtahLINK are consistent with this policy. The State Office shall be the final authority on use of the Network and the issuance of public education user accounts**;**

XI. Each school district and school shall define and adopt an Acceptable Use Policy that identifies the standards and guidelines that are appropriate to their local circumstances. However these local policies may not permit uses that are outside of the guidelines of this policy;

XII. All accounts for the school professionals within a district will be issued and managed by the local node administrator(s). The issuing of these accounts will be coordinated with the UEN Network Operations Center;

XIII. Extensive use of the network for private or personal business is prohibited;

XIV. This is a legally binding document and careful consideration shall be given to the principles outlined herein;

XV. Violations of the provisions stated in this policy may result in suspension or revocation of network privileges.

*** Such prescribed circumstances and uses shall be defined in writing by the Utah department of Education and from time to time are subject to change.**

Guidelines for Student Accounts on Utah's Public Education Network

The primary purpose of the UtahLINK is for the use of the public school professional staff and secondary student access. The use of an individual student account is considered to be a privilege and is permitted to the extent that available resources allow.

Secondary students may be granted an account for up to one academic year at a time provided they:

- Read and agree to follow all guidelines outlined in the Acceptable Use Policy. This agreement is formalized through their signature on the application form;
- Have at least one teacher sign the application form as a sponsor;
- Obtain the signature of a parent on the application form.

Elementary students are not allowed individual accounts. Teachers of these grades may apply for a class account, but are obligated to directly teach these students in proper network use and supervise them regarding the Acceptable Use Policy. * The teacher holding this account is ultimately responsible for use of the account and is required to maintain confidentiality with the password (not giving it to students) and is advised to change the passwequently.

Students may not maintain accounts upon graduation unless they otherwise qualify under one of the other acceptable use provisions. Generally, students are not permitted to enter professional UtahLINK or Usenet discussion groups. Under certain conditions, posting privileges to specific news groups may be granted. All public school student accounts will be issued by the local node administrators and will receive final approval by the State Office of Education.

The above-mentioned use is subject to revision in policy. In all cases, use by professional public education staff shall take precedence. The State Office of Education reserves its right as final authority on use of the network.

§ 54.1716 Children's Internet Protection Act Certifications.

(a) Definitions -

(1) School. For the purposes of the certification requirements of this section, school means school, school board, school district, local education agency or other authority responsible for administration of a school.

(2) Library. For the purposes of the certification requirements of this section, library means library, library board or authority responsible for administration of a library.

(3) Billed entity. Billed entity is defined in § 54.1700. In the case of a consortium, the billed entity is the lead member of the consortium.

(4) Connected devices. Connected devices are defined in § 54.1700.

(b) Who is required to make certifications?

(1) A school or library that receives support for internet access, internet service, or internal connections services under the Federal universal service support mechanism for schools and libraries, or internet access or internet service through the Emergency Connectivity Fund, must make such certifications as described in paragraph (c) of this section. The certifications required and described in paragraph (c) of this section must be made in each funding year.

(2) A school or library that receives support for connected devices through the Emergency Connectivity Fund and uses internet access or internet service funded through the Federal universal service support mechanism for schools and libraries or through the Emergency Connectivity Fund must make the certifications as described in paragraph (c) of this section. The certifications required and described in paragraph (c) of this section must be made in each funding year.

(3) Schools and libraries that are not receiving support for internet access, internet service, or internal connections under the Federal universal service support mechanism for schools and libraries; internet access or internet service through the Emergency Connectivity Fund; or connected devices that do not use internet access or internet service funded through the Federal universal service support mechanism for schools and libraries or the Emergency Connectivity Fund are not subject to the requirements in 47 U.S.C. 254(h) and (l), but must indicate, pursuant to the certification requirements in paragraph (c) of this section, that they are not receiving support for such services or that the connected devices do not use internet access or internet service funded through the Federal universal service support mechanism for schools and libraries or the Emergency Connectivity Fund.

(c) Certifications required under 47 U.S.C. 254(h) and (1) .

(1) An Emergency Connectivity Fund applicant need not complete additional Children's Internet Protection Act (CIPA) compliance certifications if the applicant has already certified its CIPA compliance for the relevant funding year (i.e., has certified its compliance in an FCC Form 486 or FCC Form 479).

(2) Emergency Connectivity Fund applicants that have not already certified their CIPA compliance for an E-Rate application for the relevant funding year (i.e., have not completed a FCC Form 486 or FCC Form 479), will be required to certify:

(i) That they are in compliance with CIPA requirements under sections 254(h) and (l);

(ii) That they are undertaking the actions necessary to comply with CIPA requirements as part of their request for support through the Emergency Connectivity Fund; or

(iii) If applicable, that the requirements of CIPA do not apply, because the applicant is not receiving support for internet access, internet service, or internal connections under the Federal universal service support mechanism for schools and libraries or internet access or internet service through the Emergency Connectivity Fund, or the connected devices do not use internet access or internet service funded through the Federal universal support mechanism for schools and libraries or the Emergency Connectivity Fund.

(d) Failure to provide certifications -

(1) Schools and libraries. A school or library that knowingly fails to submit certifications as required by this section shall not be eligible for support through the Emergency Connectivity Fund until such certifications are submitted.

(2) Consortia. A billed entity's knowing failure to collect the required certifications from its eligible school and library members or knowing failure to certify that it collected the required certifications shall render the entire consortium ineligible for support through the Emergency Connectivity Fund.

(3) Reestablishing eligibility. At any time, a school or library deemed ineligible for equipment and services under the Emergency Connectivity Fund because of failure to submit certifications required by this section may reestablish eligibility for support by providing the required certifications to the Administrator and the Commission.

(e) Failure to comply with the certifications -

(1) Schools and libraries. A school or library that knowingly fails to comply with the certifications required by this section must reimburse any funds and support received under the Emergency Connectivity Fund for the period in which there was noncompliance.

(2) Consortia. In the case of consortium applications, the eligibility for support of consortium members who comply with the certification requirements of this section shall not be affected by the failure of other school or library consortium members to comply with such requirements.

(3) Reestablishing compliance. At any time, a school or library deemed ineligible for support through the Emergency Connectivity Fund for failure to comply with the certification requirements of this section and that has been directed to reimburse the program for support received during the period of noncompliance may reestablish compliance by complying with the certification requirements under this section. Upon submission to the Commission of a certification or other appropriate evidence of such remedy, the school or library shall be eligible for support through the Emergency Connectivity Fund.

(f) Waivers based on state or local procurement rules and regulations and competitive bidding requirements.

Waivers shall be granted to schools and libraries when the authority responsible for making the certifications required by this section cannot make the required certifications because its state or local procurement rules or regulations or competitive bidding requirements prevent the making of the certification otherwise required. The waiver shall be granted upon the provision, by the authority responsible for making the certifications on behalf of schools or libraries, that the schools or libraries will be brought into compliance with the requirements of this section before the close of the relevant funding year.

7.4 LEA DATA GOVERNANCE PLANS & EMPLOYEE NON-DISCLOSURE AGREEMENT

PINNACLE SCHOOLS ADOPTED LEA DATA GOVERNANCE PLAN

1. **PURPOSE**

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data; from acquisition, to use, to disposal. Pinnacle Schools takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's

Student Data Protection Act (SDPA), U.C.A §53A-1-1401 requires that Pinnacle Schools adopt a Data Governance Plan.

2. SCOPE AND APPLICABILITY

This policy is applicable to all employees, temporary employees, and contractors of the Agency. The policy must be used to assess agreements made to disclose data to third-parties . This policy must also be used to assess the risk of conducting business. In accordance with Agency policy and procedures, this policy will be reviewed and adjusted on an annual basis or more frequently, as needed. This policy is designed to ensure only authorized disclosure of confidential information. The following 8 subsections provide data governance policies and processes for Pinnacle Schools:

1. Data Advisory Groups
2. Non-Disclosure Assurances for Employees
3. Data Security and Privacy Training for Employees
4. Data Disclosure
5. Data Breach
6. Record Retention and Expungement
7. Data Quality
8. Transparency

Furthermore, this Pinnacle Schools' Data Governance Plan works in conjunction with the Agency Information Security Policy, which:

- Designates Pinnacle Schools as the steward for all confidential information maintained within Pinnacle Schools.
- Designates Data Stewards access for all confidential information.
- Requires Data Stewards to maintain a record of all confidential information that they are responsible for.
- Requires Data Stewards to manage confidential information according to this policy and all other applicable policies, standards and plans.
- Complies with all legal, regulatory, and contractual obligations regarding privacy of Agency data. Where such requirements exceed the specific stipulation of this policy, the legal, regulatory, or contractual obligation shall take precedence.
- Provides the authority to design, implement, and maintain privacy procedures meeting Pinnacle Schools standards concerning the privacy of data in motion, at rest and processed by related information systems.
- Ensures that all Pinnacle Schools board members, employees, contractors, and volunteers comply with the policy and undergo annual privacy training.
- Provides policies and process for
    - Systems administration,
    - Network security,
    - Application security,
    - Endpoint, server, and device Security
    - Identity, authentication, and access management,
    - Data protection and cryptography
    - Monitoring, vulnerability, and patch management
    - High availability, disaster recovery, and physical protection
    - Incident Responses
    - Acquisition and asset management, and
    - Policy, audit, e-discovery, and training.

3. DATA ADVISORY GROUPS

3.1 Structure

Pinnacle has a three-tiered data governance structure to ensure that data is protected at all levels of Utah's educational system.

3.2 Group Membership

Membership in the groups require board approval. Group membership is for two years. If individual members exit the group prior to fulfilling their two-year appointment, the board may authorize Pinnacle's CAO to appoint a replacement member.

3.3 Individual and Group Responsibilities

The following outlines individual Pinnacle Schools staff and advisory group responsibilities.

LEA STUDENT DATA MANAGER RESPONSIBILITIES

1. Authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity.
2. Act as the primary local point of contact for the state student data officer.
3. A student data manager may share personally identifiable student data that are:
   a. of a student with the student and the student's parent
   b. required by state or federal law
   c. in an aggregate form with appropriate data redaction techniques applied
   d. for a school official
   e. for an authorized caseworker or other representative of the Dept. of Human Services or the Juvenile Court
   f. in response to a subpoena issued by a court.
   g. directory information
   h. submitted data requests from external researchers or evaluators,
4. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation.
5. Create and maintain a list of all LEA staff that have access to personally identifiable student data.
6. Ensure annual LEA level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas

4. EMPLOYEE NON-DISCLOSURE ASSURANCES

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

4.1 Scope

All *Pinnacle Schools* board members, employees, contractors and volunteers must sign and obey the *Pinnacle Schools* Employee Non-Disclosure Agreement (See Appendix A), which describes the permissible uses of state technology and information

4.2 Non-Compliance

Non-compliance with the agreements shall result in consequences up to and including removal of access to *Pinnacle Schools* network; if this access is required for employment, employees and contractors may be subject to dismissal.

4.3 Non-Disclosure Assurances

All student data utilized by *Pinnacle Schools* is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This policy outlines the way *Pinnacle Schools* staff is to utilize data and protect personally identifiable and confidential information. A signed agreement form is required from all *Pinnacle Schools* staff to verify agreement to adhere to/abide by these practices and will be maintained in *Pinnacle Schools* Human Resources. All *Pinnacle Schools* employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.
2. Complete a Security and Privacy Training for Researchers and Evaluators, if your position is a research analyst or if requested by the Chief Privacy Officer.
3. Consult with *Pinnacle Schools* internal data owners when creating or disseminating reports containing data.
4. Use password-protected state-authorized computers when accessing any student-level or staff-level records.
5. NOT share individual passwords for personal computers or data systems with anyone.
6. Log out of any data system/portal and close the browser after each use.
7. Store sensitive data on appropriate-secured locations. Unsecured access and flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
8. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at *Pinnacle Schools* when disposing of such records.
9. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records shall be used for such presentations.
10. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix B (Protecting PII in Public Reporting).
11. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, re-coding, blurring, perturbation, etc.
12. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
13. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data the Student Data Privacy Manager shall be consulted..
14. Use secure methods when sharing or transmitting sensitive data. The approved method is *Pinnacle Schools* 's Secure File Transfer Protocol (SFTP) website. Also, sharing within secured server folders is appropriate for *Pinnacle Schools* internal file transfer.
15. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.
16. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

4.4 Data Security and Privacy Training

4.4.1 Purpose

Pinnacle Schools will provide a range of training opportunities for all *Pinnacle Schools* staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

4.4.2 Scope

All *Pinnacle Schools* board members, employees, and contracted partners.

4.4.3 Compliance

New employees that do not comply may not be able to use *Pinnacle Schools* networks or technology.

4.4.4 Policy

1. Within the first week of employment, all *Pinnacle Schools* board members, employees, and contracted partners must sign and follow the *Pinnacle Schools* Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. New employees that do not comply may not be able to use *Pinnacle Schools* networks or technology. Within the first week of employment, all *Pinnacle Schools* board members, employees, and contracted partners also must sign and obey the *Pinnacle Schools* Employee Non-Disclosure Agreement, which describes appropriate uses and the safeguarding of student and educator data.
3. All current *Pinnacle Schools* board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum within 60 days of the adoption of this rule.
4. *Pinnacle Schools* requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data. The Chief Privacy Officer will identify these groups. Data and Statistics Coordinator will determine the annual training topics for these targeted groups based on *Pinnacle Schools* training needs.
5. Participation in the training as well as a signed copy of the Employee Non-Disclosure Agreement will be annually monitored by supervisors. Supervisors and the board secretary will annually report all *Pinnacle Schools* board members, employees, and contracted partners who do not have these requirements completed to the IT Security Manager.

5. DATA DISCLOSURE

5.1 Purpose

Providing data to persons and entities outside of the *Pinnacle Schools* increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This policy establishes the protocols and procedures for sharing data maintained by *Pinnacle Schools*. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99 and Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401.

5.2 Policy For Disclosure of Personally Identifiable Information (PII)

5.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by *Pinnacle Schools* are provided to *Pinnacle Schools* by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), LEAs will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. LEAs and *Pinnacle Schools* is not required to provide data that it does not maintain, nor is *Pinnacle Schools* required to create education records in response to an eligible student's request.

5.2.2 Third Party Vendor

Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with *Pinnacle Schools* must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may not be allowed to enter into future contracts with *Pinnacle Schools* without third-party verification that they are compliant with federal and state law, and board rule.

5.2.3 Internal Partner Requests

Internal partners to *Pinnacle Schools* include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented in *{INSERT LEA NAME HERE}*'s data request ticketing system

5.2.4 Governmental Agency Requests

Pinnacle Schools may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state

- Reporting requirement
- Audit
- Evaluation

The Coordinator of Data and Statistics will ensure the proper data disclosure avoidance are included if necessary. An Interagency Agreement must be reviewed by legal staff and must include "FERPA-Student Level Data Protection Standard Terms and Conditions or Required Attachment Language."

5.3 POLICY FOR EXTERNAL DISCLOSURE OF NON-PERSONALLY IDENTIFIABLE INFORMATION (PII)

5.3.1 Scope

External data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

5.3.2 Student Data Disclosure Risk Levels

Pinnacle Schools has determined four levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High. The Coordinator of Data and Statistics will make final determinations on classification of student data requests risk level.

5.3.2.1 Low-Risk Data Request Process

Definition: High-level aggregate data

Examples:
- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

Process:

Requester creates a ticket, Data Request forwarded to appropriate Data Steward. Data Steward fulfills requests and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket.

5.3.2.2 High-Risk Data Request Process

Definition: High-level aggregate data

Examples:
- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

Process:

Requester creates a ticket, Data Request forwarded to Data and Statistic Coordinator for review. If the request is approved, an MOA is drafted and sent to legal, placed on the board consent calendar, reviewed by the CAO, sent to the Purchasing/Contract Manager, sent to Coordinator or Data and Statistics, appropriate Data Steward fulfills the request, de-identifies data as appropriate, and sends to another Data Steward for Quality Assurance (ensuring student data protection). If it passes QA, data is sent to the requester and saves the dataset in a secure folder managed by the Coordinator of Data and Statistics. The Data Steward closes the ticket. If it does not pass QA, the data is sent back to the Data Steward for modification.

5.4 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Coordinator of Data and Statistics will ensure the proper data are shared with external researchers or evaluators to comply with federal, state, and board rules.

Pinnacle Schools may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researchers or evaluators for projects unrelated to federal or state requirements if:

1. A *Pinnacle Schools* Director, CAO, or board member sponsors an external researcher or evaluator request
2. Student data are not PII and are de-identified through disclosure avoidance techniques and other pertinent techniques as determined by the Coordinator of Data and Statistics.
3. Researchers and evaluators supply the *Pinnacle Schools* a copy of any publication or presentation that uses *Pinnacle Schools* data 10 business days prior to any publication or presentation.

6. DATA BREACH

6.1 Purpose

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

6.2 Policy

Pinnacle Schools shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, *Pinnacle Schools* staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, *Pinnacle Schools* shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

Concerns about security breaches must be reported immediately to the IT security manager who will collaborate with appropriate members of the *Pinnacle Schools'* executive team to determine whether a security breach has occurred. If the *Pinnacle Schools'* data breach response team determines that one or more employees or contracted partners have substantially failed to comply with *Pinnacle Schools*'s Agency IT Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Manager must be reported immediately to the CAO.

Pinnacle Schools will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach. *Pinnacle Schools* will make these resources available on its website.

7. RECORD RETENTION AND EXPUNGEMENT

7.1 Purpose

Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

7.2 Scope

Pinnacle Schools board member and staff.

7.3 Policy

The *Pinnacle School*s staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

In accordance with 53A-1-1407, the *Pinnacle Schools* shall expunge student data that is stored upon request of the student if the student is at least 23 years old. The *Pinnacle Schools* may expunge medical records and behavioral test assessments. *Pinnacle Schools* will not expunge student records of grades, transcripts, a record of the student's enrollment or assessment information. *Pinnacle Schools* staff will collaborate with Utah State Archives and Records Services in updating data retention schedules.

Pinnacle Schools maintained student-level discipline data will be expunged after three years.

8. QUALITY ASSURANCE AND TRANSPARENCY REQUIREMENTS

8.1 Purpose

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality at is addressed in five areas:

8.1.1 Data Governance Structure

The *Pinnacle Schools* data governance policy is structured to encourage the effective and appropriate use of educational data. The *Pinnacle Schools* data governance structure centers on the idea that data is the responsibility of all *Pinnacle Schools* sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

8.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the *Pinnacle Schools* communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation. The *Pinnacle Schools* also communicates with LEA IT staff regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Where possible, *Pinnacle Schools* program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.

On the data reporting side, the production and presentation layers provide standard data definitions and business rules. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data and Statistics produces documentation, training and FAQs on key statistics and reports, such as AYP, graduation rate and class size.

8.1.3 Data Collection

Data elements shall be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.

For all new data collections, *Pinnacle Schools* provides to the LEAs clear guidelines for data collection and the purpose of the data request. The *Pinnacle Schools* also notifies LEAs as soon as possible about future data collections. Time must be given to LEAs in order for them to begin gathering the data needed.

8.1.4 Data Auditing

Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

8.1.5 Quality Control Checklist

Checklists have been proven to increase quality (See Appendix C). Therefore, before releasing high-risk data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

9. DATA TRANSPARENCY

Annually, *Pinnacle Schools* will publicly post:

- *Pinnacle Schools* data collections
- Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

10. **PINNACLE SCHOOLS EMPLOYEE NON-DISCLOSURE AGREEMENT** (see next page)

PINNACLE SCHOOLS EMPLOYEE NON-DISCLOSURE AGREEMENT

(Initial on all blanks provided)

As an employee of the *Pinnacle Schools*, I hereby affirm that:

_____ I have read the Employee Non-Disclosure Assurances attached to this agreement form and read and reviewed Data Governance Plan *Pinnacle Schools* policies. These assurances address general procedures, data use/sharing, and data security.

_____ I will abide by the terms of the *Pinnacle Schools*' policies and its subordinate process and procedures;

_____ I grant permission for the manual and electronic collection and retention of security related information, including but not limited to photographic or videotape images of your attempts to access the facility and/or workstations.

Trainings

_____ I have completed *Pinnacle Schools* Data Security and Privacy Fundamentals Training.

_____ I will complete *Pinnacle Schools* Data Security and Privacy Fundamentals Training within 30 days.

Using Pinnacle Schools Data and Reporting Systems

_____ I will use a password-protected computer when accessing data and reporting systems, viewing child/staff records, and downloading reports.

_____ I will not share or exchange individual passwords, for either personal computer(s) or *Pinnacle Schools* system user accounts, with *Pinnacle Schools* staff or participating program staff.

_____ I will log out of and close the browser after each use of *Pinnacle Schools* data and reporting systems.

_____ I will only access data in which I have received explicit written permissions from the data owner.

_____ I will not attempt to identify individuals, except as is required to fulfill job or volunteer duties, or to publicly release confidential data;

Handling Sensitive Data

_____ I will keep sensitive data on password-protected state-authorized computers.

_____ I will keep any printed files containing personally identifiable information in a locked location while unattended.

_____ I will not share child/staff-identifying data during public presentations, webinars, etc. I understand that dummy records shall be used for such presentations.

_____ I will delete files containing sensitive data after working with them from my desktop, or move them to a secured *Pinnacle Schools* server.

Reporting & Data Sharing

_____ I will not re-disclose or share any confidential data analysis except to other authorized personnel without *Pinnacle Schools'* expressed written consent.

_____ I will not publicly publish any data without the approval of the CAO.

_____ I will take steps to avoid disclosure of personally identifiable information in state-level reports, such as aggregating, data suppression, rounding, re-coding, blurring, perturbation, etc.

_____ I will not use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If I receive an email containing such information, I will delete the screenshots/text when forwarding or replying to these messages.

_____ I will not transmit child/staff-level data externally unless explicitly authorized in writing.

_____ I understand that when sharing child/staff-identifying data with authorized individuals, the only approved methods are phone calls or *Pinnacle Schools*'s Secure File Transfer Protocol (SFTP). Also, sharing within secured server folders is appropriate for *Pinnacle Schools* internal file transfer.

_____ I will immediately report any data breaches, suspected data breaches, or any other suspicious activity related to data access to my supervisor and the *Pinnacle Schools* Information Security Officer. Moreover, I acknowledge my role as a public servant and steward of child/staff information, and affirm that I will handle personal information with care to prevent disclosure.

Consequences for Non-Compliance

_____ I understand that access to the *Pinnacle Schools* network and systems can be suspended based on any violation of this contract or risk of unauthorized disclosure of confidential information;

_____ I understand that failure to report violation of confidentiality by others is just as serious as my own violation and may subject me to personnel action, including termination.

Termination of Employment

_____ I agree that upon the cessation of my employment from *Pinnacle Schools*, I will not disclose or otherwise disseminate any confidential or personally identifiable information to anyone outside of *Pinnacle Schools* without the prior written permission of the Student Data Manager of *Pinnacle Schools*.

EMPLOYEE PRINTED NAME **EMPLOYEE SIGNATURE** **DATE SIGNED**

11. PROTECTING PII IN PUBLIC RECORDS

DATA GATEWAY STATISTICAL REPORTING METHOD FOR PROTECTING PII

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by the *Pinnacle Schools* (*Pinnacle Schools*) and local education agencies (LEAs) is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

This is done by applying the following statistical method for protecting PII.

1. Underlying counts for groups or subgroups totals are not reported.
2. If a reporting group has 1 or more subgroup(s) with 10 or fewer students.
    a. The results of the subgroup(s) with 10 or fewer students are re-coded as "N<10"
    b. For remaining subgroups within the reporting group
3. For subgroups with 300 or more students, apply the following suppression rules.
    a. Values of 99% to 100% are re-coded to ≥99%
    b. Values of 0% to 1% are re-coded to ≤1%
4. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
    a. Values of 98% to 100% are re-coded to ≥98%
    b. Values of 0% to 2% are recoded to ≤2%
5. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
    a. Values of 95% to 100% are re-coded to ≥95%
    b. Values of 0% to 5% are recoded to ≤5%
6. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
    a. Values of 90% to 100% are re-coded to ≥90%
    b. Values of 0% to 10% are re-coded to ≤10%
    c. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)
7. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.
    a. Values of 80% to 100% are re-coded to ≥80%
    b. Values of 0% to 20% are recoded to ≤20%
    c. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

12. EXAMPLE QUALITY CONTROL CHECKLIST

Reliability (results are consistent)

1. Same definitions were used for same or similar data previously reported **or** it is made very clear in answering the request how and why different definitions were used
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another *Pinnacle Schools* data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

1. Request was clarified
2. Identified and included all data owners that would have a stake in the data used

3. Data owners approve of data definitions and business rules used in the request
4. All pertinent business rules were applied
5. Data answers the intent of the request (intent ascertained from clarifying request)
6. Data answers the purpose of the request (audience, use, etc.)
7. Limits of the data are clearly stated
8. Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

1. Is date-stamped
2. Small n-sizes and other privacy issues are appropriately handled
3. Wording, spelling and grammar are correct
4. Data presentation is well organized and meets the needs of the requester
5. Data is provided in a format appropriate to the request
6. A typical person could not easily misinterpret the presentation of the data

13. USBE BOARD RULE - R277-487-4. Retention of Student Data (Approved 4/21/21)

An LEA shall retain and dispose of all student data in accordance with an approved retention schedule.

- An LEA's retention schedules shall take into account the LEA's administrative need for the data
- Unless the data requires permanent retention, an LEA's retention schedules shall require destruction or expungement of student data after the administrative need for the data has passed.

This FERPA Notice for Directory Information notice is posted on the Pinnacle's school webpage (www.pcaschool.com):

Educational Rights and Privacy Act (FERPA)
Notice for Directory Information

The *Family Educational Rights and Privacy Act* (FERPA), a Federal law, requires that Pinnacle Canyon Academy (PCA), with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, PCA may disclose appropriately designated "directory information" without written consent, unless you have advised PCA to the contrary in accordance with PCA's procedures. The primary purpose of directory information is to allow the PCA to include information from your child's education records in certain school publications. Examples include:

- A playbill, showing your student's role in a drama production;
- The annual yearbook;
- Honor roll or other recognition lists;
- Graduation programs; and
- Sports activity sheets, such as for wrestling, showing weight and height of team members.

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965, as amended (ESEA) to provide military recruiters and institutes of higher education, upon request, with the following information – names, addresses and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent. [Note: These laws are Section 9528 of the ESEA (20 U.S.C. § 7908) and 10 U.S.C. § 503(c).]

If you do not want PCA to disclose any or all of the types of information designated below as directory information from your child's education records without your prior written consent, you must notify the PCA in writing by October 1. PCA has designated the following information as directory information:

- Student's name
- Address
- Telephone listing
- Electronic mail address
- Photograph
- Date and place of birth
- Major field of study
- Dates of attendance
- Grade level
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Degrees, honors, and awards received
- The most recent educational agency or institution attended
- Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user
- A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

7.5 LEA TECHNOLOGY SECURITY POLICY

Adopted LEA Technology Security Policy
Pinnacle Schools

1. PURPOSE

The purpose of this policy is to ensure the secure use and handling of all district data, computer systems and computer equipment by District students, patrons, and employees.

2. POLICY

2.1 Technology Security

It is the policy of the *Pinnacle Schools* to support secure network systems in the district, including security for all personally identifiable information that is stored on paper or stored digitally on district-maintained computers and networks. This policy supports efforts to mitigate threats that may cause harm to the district, its students, or its employees.

The district will ensure reasonable efforts will be made to maintain network security. Data loss can be caused by human error, hardware malfunction, natural disaster, security breach, etc., and may not be preventable.
All persons who are granted access to the district network and other technology resources are expected to be careful and aware of suspicious communications and unauthorized use of district devices and the network. When

an employee or other user becomes aware of suspicious activity, he/she is to immediately contact the district's Information Security Officer with the relevant information.

This policy and procedure also covers third party vendors/contractors that contain or have access to *Pinnacle Schools* critically sensitive data. All third party entities will be required to sign the Restriction on Use of Confidential Information Agreement before accessing our systems or receiving information.

It is the policy of *Pinnacle Schools* to fully conform with all federal and state privacy and data governance laws. Including the Family Educational Rights and Privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), the Government Records and Management Act U.C.A. §62G-2 (hereinafter "GRAMA"), U.C.A. §53A-1-1401 et seq and Utah Administrative Code R277-487.

Professional development for staff and students regarding the importance of network security and best practices are included in the procedures. The procedures associated with this policy are consistent with guidelines provided by cyber security professionals worldwide and in accordance with Utah Education Network and the Utah State Office of Education. *Pinnacle Schools* supports the development, implementation and ongoing improvements for a robust security system of hardware and software that is designed to protect *Pinnacle Schools*' data, users, and electronic assets.

3. PROCEDURE

3.1. Definitions:

3.1.1. Access: Directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, computer network, or any means of communication with any of them.
3.1.2. Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner to give consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission.
3.1.3. Computer: Any electronic device or communication facility that stores, retrieves, processes, or transmits data.
3.1.4. Computer system: A set of related, connected or unconnected, devices, software, or other related computer equipment.
3.1.5. Computer network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.
3.1.6. Computer property: Includes electronic impulses, electronically produced data, information, financial instruments, software, or programs, in either machine or human readable form, any other tangible or intangible item relating to a computer, computer system, computer network, and copies of any of them.
3.1.7. Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission.
3.1.8. Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
3.1.9. Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered Protected data
3.1.10. Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons.
3.1.11. Sensitive data: Data that contains personally identifiable information.
3.1.12. System level: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

3.2. Security Responsibility

3.2.1. *Pinnacle Schools* shall appoint, in writing, an IT Security Officer (ISO) responsible for overseeing District-wide IT security, to include development of District policies and adherence to the standards defined in this document.

3.3 Training

3.3.1. *Pinnacle Schools*, led by the ISO, shall ensure that all District employees having access to sensitive information undergo annual IT security training which emphasizes their personal responsibility for protecting student and employee information. - Training resources will be provided to all District employees.
3.3.2. *Pinnacle Schools*, led by the ISO, shall ensure that all students are informed of Cyber Security Awareness.

3.4. Physical Security

3.4.1. Computer Security
3.4.1.1. *Pinnacle Schools* shall ensure that any user's computer must not be left unattended and unlocked, especially when logged into sensitive systems or data including student or employee information. Automatic log off, locks and password screensavers shall be used to enforce this requirement.
3.4.1.2. *Pinnacle Schools* shall ensure that all equipment that contains sensitive information will be secured to deter theft.
3.4.2. Server/Network Room Security
3.4.2.1. *Pinnacle Schools* shall ensure that server rooms and telecommunication rooms/closets are protected by appropriate access control which segregates and restricts access from general school or District office areas. Access control shall be enforced using either keys, electronic card readers, or similar method with only those IT or other staff members having access necessary to perform their job functions are allowed unescorted access.
3.4.2.2. Telecommunication rooms/closets may only remain unlocked or unsecured when because of building design it is impossible to do otherwise or due to environmental problems that require the door to be opened.
3.4.3. Contractor access
3.4.3.1. Before any contractor is allowed access to any computer system, server room, or telecommunication room the contractor will need to present a company issued identification card, and his/her access will need to be confirmed directly by the authorized employee who issued the service request or by *Pinnacle Schools*' Technology Department.

3.5. Network Security

3.5.1. Network perimeter controls will be implemented to regulate traffic moving between trusted internal (District) resources and external, untrusted (Internet) entities. All network transmission of sensitive data shall enforce encryption where technologically feasible.
3.5.2. Network Segmentation
3.5.2.1. *Pinnacle Schools* shall ensure that all untrusted and public access computer networks are separated from main district computer networks and utilize security policies to ensure the integrity of those computer networks.
3.5.2.2. *Pinnacle Schools* will utilize industry standards and current best practices to segment internal computer networks based on the data they contain. This will be done to prevent unauthorized users from accessing services unrelated to their job duties and minimize potential damage from other compromised systems.
3.5.3. Wireless Networks
3.5.3.1. No wireless access point shall be installed on *Pinnacle Schools*' computer network that does not conform with current network standards as defined by the Network Manager. Any exceptions to this must be approved directly in writing by the Information Security Officer.
3.5.3.2. *Pinnacle Schools* shall scan for and remove or disable any rogue wireless devices on a regular basis.
3.5.3.3. All wireless access networks shall conform to current best practices and shall utilize at minimal WPA encryption for any connections. Open access networks are not permitted, except on a temporary basis for events when deemed necessary.

3.5.4. Remote Access
3.5.4.1. *Pinnacle Schools* shall ensure that any remote access with connectivity to the District's internal network is achieved using the District's centralized VPN service that is protected by multiple factor authentication systems. Any exception to this policy must be due to a service provider's technical requirements and must be approved by the Information Security Officer.

3.6. Access Control

3.6.1. System and application access will be granted based upon the least amount of access to data and programs required by the user in accordance with a business need-to-have requirement.
3.6.2. Authentication
3.6.2.1. *Pinnacle Schools* shall enforce strong password management for employees, students, and contractors.
3.6.2.2. Password Creation
3.6.2.2.1. All server system-level passwords must conform to the Password Construction Guidelines posted on the *Pinnacle Schools* Technology Website.
3.6.2.3. Password Protection
3.6.2.3.1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential information.
3.6.2.3.2. Passwords must not be inserted into email messages or other forms of electronic communication.
3.6.2.3.3. Passwords must not be revealed over the phone to anyone.
3.6.2.3.4. Do not reveal a password on questionnaires or security forms.
3.6.2.3.5. Do not hint at the format of a password (for example, "my family name").
3.6.2.3.6. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
3.6.2. Authorization
3.6.2.1. *Pinnacle Schools* shall ensure that user access shall be limited to only those specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.
3.6.2.2. *Pinnacle Schools* shall ensure that user access shall be granted and/or terminated upon timely receipt, and management's approval, of a documented access request/termination.
3.6.3. Accounting
3.6.3.1. *Pinnacle Schools* shall ensure that audit and log files are maintained for at least ninety days for all critical security-relevant events such as: invalid logon attempts, changes to the security policy/ configuration, and failed attempts to access objects by unauthorized users, etc.
3.6.4. Administrative Access Controls
3.6.4.1. *Pinnacle Schools* shall limit IT administrator privileges (operating system, database, and applications) to the minimum number of staff required to perform these sensitive duties.

3.7. Incident Management

3.7.1. Monitoring and responding to IT related incidents will be designed to provide early notification of events and rapid response and recovery from internal or external network or system attacks.

3.8. Business Continuity

3.8.1. To ensure continuous critical IT services, IT will develop a business continuity/disaster recovery plan appropriate for the size and complexity of District IT operations.
3.8.2. *Pinnacle Schools* shall develop and deploy a district-wide business continuity plan which shall include as a minimum:

- Backup Data: Procedures for performing routine daily/weekly/monthly backups and storing backup media at a secured location other than the server room or adjacent facilities. As a minimum, backup media must be stored off-site a reasonably safe distance from the primary server room.
- Secondary Locations: Identify a backup processing location, such as another School or District building.

- Emergency Procedures: Document a calling tree with emergency actions to include: recovery of backup data, restoration of processing at the secondary location, and generation of student and employee listings for ensuing a full head count of all.

3.9. Malicious Software

3.9.1. Server and workstation protection software will be deployed to identify and eradicate malicious software attacks such as viruses, spyware, and malware.
3.9.2. *Pinnacle Schools* shall install, distribute, and maintain spyware and virus protection software on all district-owned equipment, i.e. servers, workstations, and laptops.
3.9.3. *Pinnacle Schools* shall ensure that malicious software protection will include frequent update downloads (minimum weekly), frequent scanning (minimum weekly), and that malicious software protection is in active state (real time) on all operating servers/workstations.
3.9.4. *Pinnacle Schools* shall ensure that all security-relevant software patches (workstations and servers) are applied within thirty days and critical patches shall be applied as soon as possible.
3.9.5. All computers must use the District approved anti-virus solution.
3.9.6. Any exceptions to section 3.9 must be approved by the Information Security Officer.

3.10. Internet Content Filtering

3.10.1. In accordance with Federal and State Law, *Pinnacle Schools* shall filter internet traffic for content defined in law that is deemed harmful to minors.
3.10.2. *Pinnacle Schools* acknowledges that technology based filters are not always effective at eliminating harmful content and due to this, *Pinnacle Schools* uses a combination of technological means and supervisory means to protect students from harmful online content.
3.10.3. In the event that students take devices home, *Pinnacle Schools* will provide a technology based filtering solution for those devices. However, the District will rely on parents to provide the supervision necessary to fully protect students from accessing harmful online content.
3.10.4. Students shall be supervised when accessing the internet and using district owned devices on school property.

3.11. Data Privacy

3.11.1. *Pinnacle Schools* considers the protection of the data it collects on students, employees and their families to be of the utmost importance.
3.11.2. *Pinnacle Schools* protects student data in compliance with the Family Educational Rights and privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (“FERPA”), the Government Records and Management Act U.C.A. §62G-2 (“GRAMA”), U.C.A. §53A-1-1401 et seq, 15 U.S. Code §§ 6501–6506 (“COPPA”) and Utah Administrative Code R277-487 (“Student Data Protection Act”).
3.11.3. *Pinnacle Schools* shall ensure that employee records access shall be limited to only those individuals who have specific access requirements necessary to perform their jobs. Where possible, segregation of duties will be utilized to control authorization access.

3.12. Security Audit and Remediation

3.13.1. *Pinnacle Schools* shall perform routine security and privacy audits in congruence with the District’s Information Security Audit Plan.
3.13.2. District personnel shall develop remediation plans to address identified lapses that conforms with the District’s Information Security Remediation Plan Template.

3.14 Employee Disciplinary Actions

Employee Disciplinary Actions shall be in accordance with applicable laws, regulations and District

policies. Any employee found to be in violation may be subject to disciplinary action up to and including termination of employment with the *Pinnacle Schools*.

7.6 PINNACLE WEBSITE PRIVACY POLICY

BOARD APPROVED: October 28, 2025

1. Introduction

This privacy notice describes the practices of Pinnacle regarding the collection, use, and disclosure of personal information gathered through our website, in accordance with Utah Code 53E-9-3 and Board Rule R-277-487, and federal laws like the Family Educational Rights and Privacy Act (FERPA).

2. Information We Collect

We collect information in two ways:

- **Automatically:** When you visit our website, we may automatically collect information such as the internet address you linked from, IP address, and browser type.
- **Directly from you:** When you choose to provide it to us, such as through contact forms, online applications, or registration for events. This may include:
  - Names
  - Addresses
  - Email addresses
  - Phone numbers

3. How We Use Your Information

We use the information collected for the following purposes:

- To respond to your inquiries.
- To provide requested services or materials.
- To maintain contact lists.
- To ensure the website is working correctly and is accessible.
- To improve the website and make it more useful.
- For educational and administrative purposes as required by law.

4. How We Protect Your Information

- We have implemented security safeguards to protect your personal information from unauthorized access, loss, or alteration.
- Our website uses HTTPS to encrypt communication when sensitive data is transmitted.
- We do not sell your personal information.

5. Sharing Your Information with Third Parties

- We do not disclose personally identifiable student information unless a parent/guardian has given consent, or an exception applies.
- **Exceptions to consent include:**
  - Disclosures to third-party service providers who perform functions on our behalf, such as website hosting, but only with a contractual agreement for confidentiality.
  - Disclosures required to protect your health and safety, such as in an emergency.
  - Disclosures for legal or governmental requests.
  - Disclosures for audits or evaluations of educational programs.

6. Your Rights and Choices

- You have the right to know our policies and practices for managing personal information.
- We will provide you with notice if we plan to use your information for different purposes.

7. Contact Us

If you have any questions about our privacy practices, please contact us at: Ashley Downard, Business Manager, downarda@pantheremail.com, (435) 613-1802, www.pcaschool.com