Privacy Policy

Last Updated: September, 2024

Contact Us!

A+ Technology and Security ("Company", "we", "our" or "us") respects your privacy and is committed to protecting it through our compliance with this Privacy Policy (the "Policy"). The Sites (hereinafter defined) are intended to be a safe environment for anyone who accesses and/or uses them. This Policy describes the types of information we may collect from you or that you may provide when you visit the Company's websites located at https://www.aplustechnology.com (our "Website") or any of our social media accounts or webpages (the "Social Media Sites") and our practices for collecting, processing, using, retaining, protecting, and disclosing that information (collectively, the "Sites"). By accessing the Company's Sites, you consent to the collection, processing, use, retention, protection and disclosure of your information by the Company as described in this Policy. By accessing the Sites, you accept and agree to be bound and abide by this Policy and our Terms of Use, located at https://www.aplustechnology.com/terms-of-use/ (the "**Terms of Use**"), incorporated herein by reference. In addition, you agree to be bound by the terms and conditions, privacy policy, and/or other policies (the "**Social Media Platform Rules**") of any of the social media websites, platforms, and applications on which the Company's Social Media Sites reside. In addition, you agree to be bound by any other terms and conditions posted by the Company on any of the Company's Sites.

This Policy applies to the information we collect:

- on the Sites;
- in email, text, and other electronic messages between you and the Sites; and
- in telephone communications between you and the Company.

This Policy does not apply to information collected by:

- Through any other means, including on any other website operated by Company or any third party; or
- Any third party, including through any application or content (including advertising) that may link to or be accessible from or on the Sites.

Your Acceptance of this Policy

THIS POLICY REQUIRES THE USE OF ARBITRATION (ON AN INDIVIDUAL BASIS ONLY; I.E., CASE CONSOLIDATIONS AND CLASS ACTIONS ARE NOT PERMITTED) IN ORDER TO RESOLVE DISPUTES. Please read this Policy carefully to understand our policies and practices regarding your information and how we will treat it. By accessing or using any of the

Sites, you agree to this Policy. **If you do not agree to this Policy, you are directed to discontinue using and accessing the Company's Sites.** The Company reserves the right to change or update this Policy at any time and without prior notice to you. Your continued access or use of the Sites after such changes or updates indicates your acceptance of the Policy as changed or updated. It is your responsibility to review this Policy regularly for any changes or updates.

Acknowledgement of Risks

By using the Company's Sites, you acknowledge that you are aware of security and privacy limitations including but not limited to: (1) the global accessibility of the Company's Sites on the Internet; (2) the technological limitations of security, privacy, and authentication measures and features on Internet sites and specifically on the Company's Sites; (3) the risk that data or information is transmitted to or from the Company's Sites may be subject to eavesdropping, sniffing, spoofing, forgery, spamming, "impostering", tampering, breaking passwords, harassment, fraud, electronic trespassing, hacking, denial of service attacks, nuking, system contamination (including computer viruses, Trojan horses, worms, defects, date bombs, time bombs, malware, ransomware, bugs, executables or other items of a destructive nature or any other malicious computer codes, scripts, applications or programs) causing unauthorized, damaging, or harmful access to and/or retrieval of information and data on your computer or network; (4) the risk that data or information on any of the Company's Sites may be subject to other security or privacy hazards, may not reach its destination, or may reach an erroneous address or recipient; (5) unauthorized access by third parties; and (6) the content or the privacy policies of other websites, social media websites, platforms, and applications, including without limitation those to which the Company may link or be linked.

Information We Collect About You

When you use our Sites, the Company and/or our third party service providers collect certain information about you. Among the types of information from and about users of our Sites that we collect includes:

- **Identifiers**. This includes any information by which you may be personally identified, such as name, postal address, e-mail address, telephone number, account credentials, birth date, zip code, or any other identifier by which you may be contacted online or offline;

- **Commercial Information**. Such as your order information, including related transaction information such as payment method, order status, goods and/or services purchased;
- **Communications Information.** Including information that you provide during communications and interactions with us, which may include the content of email messages and phone calls. This may also include information that you provide by filling in forms on our Sites or that you otherwise Post (as such term is defined below) on the Sites. This may also include information you provide when you report a problem with

our Sites. **Internet or other Electronic Network Activity Information**. Including your Internet connection information such as your IP address, your operating system, and browser type, the equipment you use to access our Sites, unique device identifiers, cookie identifiers, web beacons, device and browser settings and information, interactions with our Sites, information about how and when you access our Sites, such as the date and time of your visit or use, the website or URL to which you go upon leaving the Sites, and other usage details.

- **Geolocation Information**. Including device information when using our Sites (if your device settings permit us to collect this information).
- **Inferences.** We may use information about or derived from the information above including technologies to collect information about your online activities over time and across third-party websites or other online services (behavioral tracking). The information we collect automatically may include personal information or we may maintain it or associate it with personal information we collect in other ways or receive from third parties. It helps us to improve our Sites and to deliver a better and more personalized service, including by enabling us to estimate our audience size and usage patterns.

(collectively, "personal information").

How We Collect Your Personal Information

We collect your personal information:

- Directly from you when you provide it to us.
- Automatically as you navigate through the Sites collected through cookies and other tracking technologies.
- From third parties, for example, our business partners.

You also may post, submit, transmit, upload or otherwise provide (hereinafter, "**Post**") information, including without limitation posts, comments and reviews to be published or displayed on the Sites, or transmitted to other users of the Sites or third parties (collectively, "**User Content**" and, together with personal information and Automatic Data (as such term is defined below), "**User Data**"). Your User Content is Posted and transmitted to others at your own risk. Although we may limit access to certain portions of the Sites, please be aware that no security measures are perfect or impenetrable. Additionally, we cannot control the actions of other users of the Sites with whom you may choose to share your User Content. Therefore, we cannot and do not guarantee that your User Content will not be viewed by unauthorized persons.

Information We Collect Through Automatic Data Collection Technologies

As you navigate through and interact with our Sites, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns (collectively, "**Automatic Data**").

The technologies we use for this automatic data collection may include:

- **Cookies (or browser cookies).** A cookie is a small file placed on the hard drive of your computer. You may refuse to accept browser cookies by activating the appropriate setting on your browser. However, if you select this setting you may be unable to access certain parts of our Website. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you direct your browser to our Website.
- **Flash Cookies.** Certain features of our Website may use local stored objects (or Flash cookies) to collect and store information about your preferences and navigation to, from, and on our Website. Flash cookies are not managed by the same browser settings as are used for browser cookies.
- **Web Beacons.** Pages of our Website may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited certain webpages and for other related statistics (for example, recording the popularity of certain content on the Website and verifying system and server integrity).
- "Cookies", "Flash Cookies" and "Web Beacons" (collectively, "**User Attribution Devices**") help facilitate and enhance the Sites' communications and interactions with you. The Company may share information collected via User Attribution Devices with third parties, including without limitation advertising, analytics and social media websites, platforms and applications, to inform, optimize and serve information and content to you, including without limitation advertisements. You may opt-out of collection and use of information by certain User Attribution Devices in connection with your use of the Sites by: (i) visiting http://optout.aboutads.info/; and/or (ii) setting your Internet browser to refuse certain types of User Attribution Devices, such as cookies.
- Some content, including without limitation advertisements, on the Sites are served by third parties, including advertisers, ad networks and servers, content providers, and application providers. These third parties may use cookies (alone or in conjunction with other User Attribution Devices) to collect information about you when you use our Sites. The information they collect may be associated with your personal information or they may collect information, including personal information, about your online activities over time and across different websites and other online services. They may use this information to provide you with interest-based (behavioral) advertising or other targeted content. We may not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

How We Use Your Information

We may use information about our users, including without limitation any User Data, in aggregated, anonymized and/or non-personally identifiable form, without restriction (except to the extent prohibited by applicable law).

We may use information that we collect about you or that you provide to us as described in this Policy, including without limitation any User Data:

- To personalize your experience on the Sites.
- To improve our customer service.
- To present our Sites and their contents to you.
- To provide you with information, products, or services that you request from us, including without limitation to provide you with updates regarding any order for products that you make.
- To fulfill any other purpose for which you provide it.
- To carry out our obligations and enforce our rights arising from any contracts entered into between you and us, including for billing and collection.
- To notify you about changes to our Sites or any products we offer or provide though it.
- To administer a contest, sweepstakes, other promotion, survey or other feature of the Sites.
- To allow you to participate in interactive features on our Website.
- To comply with legal processes and safety requirements, including to maintain the security of our customers, employees, and property, respond to court orders, lawsuits, subpoenas, and government requests, as well as to address legal and regulatory compliance purposes.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

You expressly consent to the Company using your User Data, including without limitation your name, phone number, address and email address, to contact you regarding your activities on the Sites, including without limitation regarding any transaction or review on the Sites. We may also use your User Data to contact you about Company news and updates and about our own and third parties' goods and services that may be of interest to you. We may also use the information we have collected from you to enable us to display advertisements to our advertisers' target audiences. Even though we do not disclose your personal information for these purposes without your consent, if you click on or otherwise interact with an advertisement, the advertiser may assume that you meet its target criteria.

Storage and Retention of User Data

The Company considers protecting the security of your User Data important. The Company follows generally accepted administrative, technical, and physical industry standards to protect personal information submitted to us, both during transmission and once we receive it. However, the Company cannot and does not guarantee the security of any User Data,. Unfortunately, the transmission of information via the Internet is not completely secure. You

must protect the privacy of your own information. You are solely responsible for the security of all such information at all times. You must take precautions to protect the security of all User Data that you may transmit to, from or through the Sites over any home networks, routers, private wireless (WiFi) networks, public WiFi networks, and all other communication technologies. We are not responsible for circumvention of any privacy settings or security measures contained on the Sites, for the unauthorized acts of others, or for acts or omissions beyond our reasonable control.

Your personal information and all User Data are stored by the Company on its servers, and on the servers of the cloud-based database management services the Company engages, located in the United States. We will retain your User Data for as long as you remain a customer, for which we need to hold your User Data to deliver our products and services to you, and for a period of time thereafter as long as necessary for legal reasons or to protect our interests. For more information about how long your User Data is stored, and for more information on your rights for erasure or portability, please contact us at info@aplustechnology.com.

Third Parties and Information We Disclose

Other than as set forth above and discussed in this section, we will not collect or use your User Data when you use our Sites, unless you choose to provide such information to us, nor will such information be sold or otherwise transferred to unaffiliated third parties without your approval at the time of collection.

We may disclose any information about our users, including without limitation any User Data, in aggregated, anonymized and/or non-personally identifiable form, without restriction (except to the extent prohibited by applicable law).

We may disclose information that we collect about you or that you provide to us as described in this Policy, including without limitation any User Data:

- To our subsidiaries and affiliates.
- To contractors, service providers, and other third parties we use to support our business and who are bound by contractual obligations to keep the information that we disclose about you confidential and use it only for the purposes for which we disclose it to them.
- To a subsidiary, affiliate, buyer, or other successor in the event of a merger, divestiture, restructuring, consolidation, reorganization, dissolution, or other sale or transfer of some or all of Company's assets, whether as a going concern or as part of bankruptcy, insolvency, liquidation, or similar proceeding, in which information held by the Company about you is among the assets transferred.
- To third parties to market their products or services to you if you have not opted out of these disclosures.
- To fulfill the purpose for which you provide it.
- For any other purpose disclosed by us when you provide the information.

- Otherwise with your consent.

Your Choices About How We Use and Disclose Your Information

To process your User Data, we rely upon your consent, contract performance, our legitimate business interest, or compliance with law. You may object or restrict our processing of your User Data. You may withdraw any prior consent you may have given to process your User Data at any time. It is also within your rights to refuse to provide any User Data we request. However, refusal to provide certain User Data may limit your access to information or use of the Sites.

Should you wish to access or amend any User Data you may have provided to us or if you wish to request deletion, please contact info@aplustechnology.com.

You may also exercise the following controls over your User Data:

- **Tracking Technologies and Advertising.** You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent. To learn how you can manage your Flash cookie settings, visit the Flash player settings page on Adobe's website located at: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html. If you disable or refuse cookies, please note that some parts of the Sites may then be inaccessible or not function properly.
- **Promotional Offers from the Company.** If you do not wish to have your email address used by the Company to promote our own or third parties' products or services, you can opt-out by sending us an email stating your request to info@aplustechnology.com. If we have sent you a promotional email, you may send us a return email asking to be omitted from future email distributions. This opt-out does not apply to information provided to the Company as a result of a product purchase or other related transactions.

In any such case of your withdrawal of consent, you acknowledge that there may be a delay before the Company fully implements your request and you may therefore still be contacted by the Company for a period of time thereafter. Notwithstanding your withdrawal of consent, the Company may subsequently contact you for other purposes that are unrelated to marketing and/or selling, including without limitation legal or regulatory purposes. Please be aware that applicable laws, statues, rules and/or regulations may require or permit the collection, processing, retention, use and disclosure of your User Data without your consent. Notwithstanding the foregoing, pursuant to applicable laws, statues, rules and/or regulations or other reasons, there may be circumstances in which you may not withdraw your consent to the collection, processing, use, retention and disclosure of your User Data.

We do not control third parties' collection or use of your information to serve interest-based advertising. However, these third parties may provide you with ways to choose not to have your information collected or used in this way. You can opt out of receiving targeted ads from

members of the Network Advertising Initiative ("**NAI**") on the NAI's website located at http://optout.networkadvertising.org/?c=1.

Most Internet browsers can be set to transmit digital "Do Not Track" requests to websites. Such sites may but are not required to comply with "Do Not Track" requests. At this time, the Website does not respond to any digital "Do Not Track" requests.

The Company's Social Media Sites

The Company maintains accounts and sites on third party social media websites, platforms and applications including without limitation, Facebook, Twitter, LinkedIn and YouTube. Your use of the Company's Social Media Sites shall be subject to all of the following: this Policy; the Terms of Use; and the terms of use, privacy policy, and all other applicable terms and conditions for each social media website, platform and application on which the Company's Social Media Sites reside, as in effect at such time.

In addition, when you register to use social media websites and platforms in general, you are generally required to furnish profile and other information to such websites and platforms in accordance with their own internal policies. Therefore, by using the Company's Social Media Sites, you authorize the Company to collect and retain information about you, including your profile and other information you disclosed to such social media websites, platforms and applications and other information arising from your access and use of the Company's Social Media Sites. You expressly consent to the Company's collection, processing, retention, use and disclosure of such information in accordance with this Policy and the Terms of Use.

Children

The Website is not marketed to or intended for users under the age of eighteen (18). No one under the age eighteen (18) may provide any personal information, or User Data, to or on the Website. The Company is committed to the safety of children and to protecting the online privacy of children. The Company does not request or knowingly collect any User Data from children under the age of eighteen. If you believe we might have any information from or about a child under the age of eighteen, please contact us at info@aplustechnology.com.

Rights of Certain Types of Users

Subject to applicable law, you may have certain rights with regard to your User Data. These rights may include the following rights to (1) access or correct your User Data, (2) request the deletion of your User Data, (3) request to opt out of certain processing or another restriction on the processing of your User Data, (4) request a portable form of your User Data, (5) object to the processing of your User Data, or (6) exercise other rights with respect to your User Data. To learn more about the User Data we collect about you or the rights you may have, please contact us at info@aplustechnology.com.

1. **International Users**

Under the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), if you are a user residing in the European Economic Area (EEA) and the United Kingdom (UK), you have certain rights to your User Data, including the rights of access, correction, erasure, restriction, objection, and data portability, as well as the right to withdraw consent to certain processing of your User Data.

The Company's (1) legitimate interests and legal basis for processing your User Data; (2) categories of personal data we collect; and (3) storage and retention period of your User Data are set forth above. If the Company engages in any transfer of your User Data outside of the jurisdiction of collection or your residence, we will seek your consent as discussed above and/or transfer such User Data in accordance with the GDPR.

While we strongly encourage you to first raise any questions or concerns about your User Data directly with us, you may have a right to lodge a complaint with the relevant supervisory authority. To exercise any of the rights listed in this section, or to contact the Company's data protection officer, please contact us at info@aplustechnology.com.

For users residing in other international countries, if you provide us with User Data, you understand that your User Data will be transferred to and processed in the United States of America and any other country or jurisdiction at our sole discretion. The laws that apply to the use and protection of User Data in the United States or other countries or jurisdictions in which we transfer or process your User Data may be different from the laws and protections in your country. Please contact us at info@aplustechnology.com if you have any questions concerning your User Data.

California Users

If you are a California resident, California law may provide you with additional rights regarding our use of your personal information.

For business purposes for the last twelve (12) months, the Company may have collected, used, and shared User Data about you as described in this Policy. The categories of User Data that the Company may have collected and used are set forth above. California residents have the right to request a copy of, access to, make revisions, or seek deletion of their User Data. California residents may also opt out of the sale of their User Data.

California residents can also designate an authorized agent to submit requests on their behalf. We will take reasonable steps to verify your identity and the identity and authority of your authorized agent prior to complying with any request. The CCPA further provides you with the right to not be discriminated against (as provided for in applicable law) for exercising your rights. Please note that certain information may be exempt from such requests under California law.

If you are a California resident and would like to exercise any of legal rights under the CCPA, please contact us at info@aplustechnology.com.

Annually, California residents may request and obtain information about the User Data that the Company has shared with third parties for such third parties' direct marketing purposes within the prior calendar year (as defined by California Civil Code § 1798.83, commonly known as California's "Shine the Light Law"). If applicable, this information would include a list of the categories of User Data that was shared and the names and addresses of all third parties with which the Company shared this information in the immediately preceding calendar year. To obtain this information, please send an email message to info@aplustechnology.com with the words "California Shine the Light Privacy Request" in the subject line as well as in the body of your message. The Company shall then furnish any applicable requested information to your email address.

Other United States Users

For users residing in Colorado, Connecticut, Montana, Virginia, Tennessee, Texas, or Utah, and in other such states not explicitly listed, state law grants you additional rights with regard to your User Data under applicable law. You or your legally designated representative may submit a request to exercise your User Data rights by contacting us at info@aplustechnology.com.

General Terms

This Policy, the Terms of Use, and any other terms or conditions posted by the Company on any of the Company's Sites, constitute the entire agreement between you and the Company with respect to the matters herein and therein and supersede all prior and contemporaneous understandings, agreements, representations, and warranties, written and oral, between the Company and you. No action or inaction by the Company shall be construed as a waiver of this Policy, the Terms of Use, or any other terms or conditions posted on any of the Company's Sites. No waiver by the Company of any term or condition in this Policy, the Terms of Use, or any other terms or conditions posted on any of the Company's Sites shall be deemed a further or continuing waiver of such term or condition or a waiver of any other term or condition. If any of the provisions of this Policy, the Terms of Use, or any other terms or conditions posted on any of the Company's Sites are held to be invalid, unenforceable or illegal, such provision shall be eliminated or limited to the minimum extent such that the validity and enforceability of the remaining provisions of this Policy, the Terms of Use, and any other terms or conditions posted on any of the Company's Sites shall not be effected thereby and shall continue in full force and effect.

Contact Information

To ask questions or comment about this Policy and our privacy practices, contact us at:

A+ Technology and Security
1490 North Clinton Avenue
Bay Shore, New York 11706

Or you may email us at: info@aplustechnology.com.

PARENT'S BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Ulster BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law §2-d, Ulster BOCES wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to:

   Ulster BOCES
   175 Route 32 North
   New Paltz, New York 12561

   or

   Chief Privacy Officer
   New York State Education Department
   89 Washington Avenue
   Albany, New York 12234

   Complaints may also be directed to the
   Chief Privacy Officer (CPO) via e-mail at
   CPO@mail. nysed.gov

6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data as well as teacher or principal data.

Supplemental Information Regarding Third Party Contractors

In the course of complying with its obligations under the law and providing educational services, Ulster BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law.

Each contract Ulster BOCES enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include the following information:

1. The exclusive purposes for which the student data or teacher or principal data will be used by third party contractor;

2. How the third party contractor will ensure that the subcontractors, persons or entities with whom the third party contractor will disclose the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

3. The duration of the contract, including when the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.

6. Address how the data will be protected using encryption while in motion and at rest.

Signature: Drew Cassara

Print Name: Drew Cassara

Title: Inside Sales Manager

Company Name: A+ Technology & Security Solutions, Inc.

Date: 9-26-2024

The following has been pulled from the Parents' Bill of Rights section in the Education Law 2-d Rider packet. Please review and answer questions 1, 2, 3 and 5.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   A+ Technology & Security Solutions, Inc. can confirm that any and all data (including student, teacher; and principal data) is not to be used/or any purpose, other than the encryption of that data.

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

   To process your User Data, we rely upon your consent, contract performance, our legitimate business interest, or compliance with law. You may object or restrict our processing of your User Data. You may withdraw any prior consent you may have given to process your User Data at any time. It is also within your rights to refuse to provide any User Data we request. However, refusal to provide certain User Data may limit your access to information or use of the Sites.

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the contract;

   We will retain your User Data for as long as you remain a customer, for which we need to hold your User Data to deliver our products and services to you, and for a period of time thereafter as long as necessary for legal reasons or to protect our interests.

4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected;

   Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security) and the security protections taken to ensure that such data will be protected, including whether such data will be encrypted.

   Your personal information and all User Data are stored by A+ Technology & Security Solutions, Inc. on the servers of the cloud-based database management services the Company engages, located in the United States.

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and A+ Technology & Security Solutions, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Ulster County BOCES ("BOCES") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that Ulster County BOCES' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by Ulster County BOCES. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of Ulster County BOCES as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of Ulster County BOCES relating to the annual professional performance reviews of classroom teachers or principals that is

confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with Ulster County BOCES policy(ies) on data security and privacy. Contractor shall promptly reimburse Ulster County BOCES for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of Ulster County BOCES' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of Ulster County BOCES' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to Ulster County BOCES, transitioned to a successor contractor, at Ulster County BOCES' option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of Ulster County BOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, BOCES board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of Ulster County BOCES' Parent Bill of Rights.

NAME OF PROVIDER: A+ Technology & Security Solutions, Inc.

BY: Drew Cassara **DATED:** **9-26-2024**

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.