



305 North Service Road
Dix Hills, NY 11746-5871
(631) 656-2163
(631) 656-2191 FAX

DUAL ENROLLMENT AGREEMENT
by and between
Commack High School and Five Towns College

Effective September 1, 2023 to June 30, 2024

WHEREAS, a dual enrollment agreement by and between Commack High School and Five Towns College (hereinafter the College) that further enhances the education opportunities available for their students is beneficial; and

WHEREAS, both Commack High School and the College seek to provide the students with the best preparation for success in their chosen vocations by, among other things, facilitating the transition to post-secondary study when appropriate, and

WHEREAS, both Commack High School and the College seek to establish a dual enrollment agreement for the benefit of students, who seek to pursue a course of study leading to an appropriate degree from College, and

WHEREAS, both Commack High School and the College seek to achieve the above-stated objectives by furthering the following goals:

- To provide an opportunity for Commack High School students to enter into a fully designated career tract, beginning at the secondary school level and progressing sequentially to an appropriate degree program;
- To foster an understanding among Commack High School students about the opportunity for post-secondary study;
- To develop students who have the potential for success and are prepared to succeed, without regard to their financial ability or economic background; and
- To develop students who value learning for its own sake, who are committed to lifelong learning, and who are able to avail themselves of educational opportunities presented by technological advances.

NOW THEREFORE, it is agreed as follows:

This agreement shall commence as of September 1, 2023, and shall remain in effect until June 30, 2024.

The College shall be responsible for:

- Providing of the designated course overviews to Commack High School to ensure these courses offered at the College are taught at the high school;
- Providing scholarship funding for students who pursue post-secondary study at the College;
- Identify opportunities for Commack High School Students to participate in the activities of the College;
- Inviting students to tour the campus; and
- Notifying Commack High School of any changes in the agreement.

Commack High School shall be responsible for:

- Planning and delivery of designated College coursework at the secondary school level;
- Providing to the College the instructor's CV and NYSED license certifications; and
- Planning the schedule of student assignments to include all of the coursework, assessments, and outcomes as indicated on the College's current *Course Overviews* for the designated courses.

In order for a Commack High School student to receive credits from the College, the student must:

- Play advanced NYSSMA music selections to receive College credit;
- Be in the Junior or Senior year to receive College credit;
- Register for the course as instructed by the Commack High School coordinator and pay a fee of \$50 administration fee directly to the College; (\$5 for those who are on a reduced lunch program);
- Successfully complete the College's curricula as detailed by this agreement and offered by Commack High School as indicated; and
- Achieve a grade of C (75%) or higher in designated courses.

Students who present the credentials set forth above to the College shall be eligible to receive credit as set forth in *Schedule A*, a copy of which is annexed hereto and made a part of hereof.

Both Commack High School and the College shall endeavor to publicize this dual enrollment agreement internally to potential students, so that these students and their families will become aware of the opportunities available to them.

This Agreement shall be governed and construed under the laws of the State of New York and the venue for any action, claim, or dispute arising hereunder shall be in Suffolk County, New York.

Notices under this Agreement shall be deemed to have been duly served if emailed to:

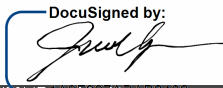
Mark Stuckey
Director of Arts & Music
Commack High School
1 Scholar Lane
Commack, NY 11725
mstuckey@commack.k12.ny.us

Either party may terminate this Agreement immediately upon written notice to the other in the event the other party is in material breach of the Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement.

By: Marsha Pollard
Marsha Pollard
Provost, Five Towns College

8/8/23
Date

By: 
Justin Varughese
President of Board of Education
Commack School District

9/8/2023
Date

FIVE TOWNS COLLEGE
Proposed Dual Enrollment Components
For Music

The following Five Towns College courses are to be suggested for credit in a dual enrollment agreement with Commack High School. Final approval is contingent upon discussion and agreement with the Chair of the FTC Music Division and the faculty of Commack High School.

1. MUS111 Harmony 1 (1 credit)
2. MUS123 Ear Training 1 (1 credit)
3. ENS374 Orchestra (1 credit)
4. ENS330 Concert Band (1 credit)
5. ENS326 Choir (1 Credit)

RIDER TO CONTRACT BETWEEN
COMMACK UNION FREE SCHOOL DISTRICT AND
FIVE TOWNS COLLEGE
EFFECTIVE SEPTEMBER 1, 2023 TO JUNE 30, 2024

To the extent that the provisions of this Rider are inconsistent with the attached contract effective September 1, 2023 to June 30, 2024 (the "Contract") to which this Rider is attached, the provisions of this Rider will control. The Contract and this Rider are collectively hereinafter referred to as the "Agreement."

1. All references to Commack High School in the Agreement will be revised with Commack Union Free School District.

2. Independent Contractor: FIVE TOWNS COLLEGE (the "Consultant") is retained by the COMMACK UNION FREE SCHOOL DISTRICT (the "District") only for the purposes and to the extent set forth in this Agreement. The Consultant's relation to the District is solely that of an independent contractor during the period of the Consultant's retention and delivery of Services hereunder.

Neither the Consultant nor any of its employees, shareholders, partners, members, officers, directors, agents, or assigns will be eligible for employee benefits or contributions thereto from the District relative to this Agreement including, but not limited to, social security, New York State Worker's Compensation, unemployment insurance, New York State Retirement System benefits, health or dental insurance, or malpractice insurance. With regard to employees of the Consultant, the Consultant alone will be responsible for their work, personal conduct, direction, compensation, and for payment of all employment and other taxes in relation thereto.

3. Indemnification: To the fullest extent permitted by law, the Consultant indemnifies and will defend (with counsel selected by the District) and hold harmless the

District, its employees, agents, representatives and members of the Board of Education, from any and all liabilities, losses, costs, damages, and expenses (including, but not limited to, reasonable attorney's fees and disbursements) arising from any claims, disputes, or causes of action of whatever nature arising, in whole or in part, from the performance of the Consultant's Services hereunder, or the action of, or the failure to act by the Consultant, the Consultant's representatives or employees, or anyone for whose acts the Consultant may be liable.

In the event that any legal proceeding is instituted or any claim or demand with respect to the foregoing is asserted by any person in respect of which indemnification may be sought from the Consultant pursuant to the provisions of this Paragraph 3, the District will promptly notify the Consultant of the legal proceeding, claim or demand, and give the Consultant an opportunity to defend and settle same without any cost to the District, and will extend reasonable cooperation to the Consultant in connection with such defense, which will be at the expense of the Consultant. In the event that the Consultant fails to defend the same within 30 calendar days of receipt of notice, the District will be entitled to assume the defense thereof, and the Consultant will be liable to repay the District for all its expenses reasonably incurred in connection with the defense (including reasonable attorney's fees, disbursements, expert witness fees and settlement payments). The failure of the District to notify the Consultant of a legal proceeding, claim or demand will not relieve the Consultant of any obligation that the Consultant has pursuant to this Paragraph unless and only to the extent that the failure to notify the Consultant materially prejudices the Consultant.

All of the provisions of this Paragraph 3 will survive the expiration or

Select Start to begin

START

sooner termination of this Agreement.

4. **Insurance:** The Consultant will obtain and keep in full force and effect during the term of this Agreement, at the Consultant's sole cost and expense, the following insurance: *Insurance waived per M. Stuckey / L. Newman – 7.19.23*

- a. **Commercial General Liability Insurance**
\$1,000,000 per occurrence/ \$2,000,000 aggregate
\$2,000,000 Products and Completed Operations
\$1,000,000 Personal and Advertising Injury
\$1,000,000 Sexual Misconduct and Assault
\$100,000 Fire Damage
\$10,000 Medical Expense
- b. **Workers' Compensation and N.Y.S. Disability**
Statutory Workers' Compensation (C-105.2 or U-26.3), Employers' Liability and N.Y.S. Disability Benefits Insurance (DB-120.1) for all employees. Proof of coverage must be on the approved specific form, as required by the New York State Workers' Compensation Board. ACORD certificates are not acceptable.

A person seeking an exemption must file a CE-200 form with the State. The form may be completed and submitted directly online to the Workers Compensation Board.
- c. **Professional Errors and Omissions Insurance**
\$2,000,000 per occurrence/ \$2,000,000 aggregate for the professional acts of the Consultant performed under this Agreement for the District. If written on a "claims-made" basis, the retroactive date must pre-date the inception of this Agreement. Coverage must remain in effect for two calendar years following the completion of work.
- d. **Excess Insurance**
\$1,000,000 each occurrence and aggregate. Excess coverage must be on a follow-form basis over the required Commercial General Liability, Automobile and Professional Errors and Omissions coverages.

Notwithstanding any terms, conditions or provisions, in any other writing between the parties, the Consultant hereby agrees to effectuate the naming of the District as

sooner termination of this Agreement.

4. **Insurance:** The Consultant will obtain and keep in full force and effect during the term of this Agreement, at the Consultant's sole cost and expense, the following insurance:

- a. **Commercial General Liability Insurance**
\$1,000,000 per occurrence/ \$2,000,000 aggregate
\$2,000,000 Products and Completed Operations
\$1,000,000 Personal and Advertising Injury
\$1,000,000 Sexual Misconduct and Assault
\$100,000 Fire Damage
\$10,000 Medical Expense
- b. **Workers' Compensation and N.Y.S. Disability**
Statutory Workers' Compensation (C-105.2 or U-26.3), Employers' Liability and N.Y.S. Disability Benefits Insurance (DB-120.1) for all employees. Proof of coverage must be on the approved specific form, as required by the New York State Workers' Compensation Board. ACORD certificates are not acceptable.

A person seeking an exemption must file a CE-200 form with the State. The form may be completed and submitted directly online to the Workers Compensation Board.

- c. **Professional Errors and Omissions Insurance**
\$2,000,000 per occurrence/ \$2,000,000 aggregate for the professional acts of the Consultant performed under this Agreement for the District. If written on a "claims-made" basis, the retroactive date must pre-date the inception of this Agreement. Coverage must remain in effect for two calendar years following the completion of work.
- d. **Excess Insurance**
\$1,000,000 each occurrence and aggregate. Excess coverage must be on a follow-form basis over the required Commercial General Liability, Automobile and Professional Errors and Omissions coverages.

Notwithstanding any terms, conditions or provisions, in any other writing between the parties, the Consultant hereby agrees to effectuate the naming of the District as an additional insured on the Consultant's insurance policies, with the exception of workers'

compensation, N.Y. State disability and professional liability. Each policy naming the District as an additional insured must:

- be an insurance policy from an A.M. Best rated “A-” or better insurer, licensed in New York State.
- state that the Consultant’s coverage is primary and non-contributory coverage for the District, its Board, employees and volunteers, committee members and student teachers as additionally insureds with no responsibility for payment of premium.

The District must be listed as an additional insured by using endorsement CG 2026 or its equivalent. The decision to accept an alternative endorsement rests solely with the District. A completed copy of the endorsement must be attached to the certificate of insurance and the certificate must state that the endorsement is being used. The certificate of insurance must describe the specific services provided by the Consultant (e.g., physical therapy, psychological services) that are covered by the commercial general liability policy and the umbrella policy. At the District's request, the Consultant will provide a copy of the declarations page of its liability and umbrella policies with a list of endorsements and forms. If so requested, the Consultant will provide a copy of the policy endorsements and forms.

The Consultant hereby indemnifies the District for any applicable deductibles and self-insured retentions, all of which are the sole responsibility of the Consultant, to the extent not covered by the applicable policy.

If a policy is written on a “claims-made” basis, the retroactive date must pre-date the inception of this Agreement.

The Consultant acknowledges that failure to obtain the foregoing insurance on behalf of the District constitutes a material breach of contract. The

Consultant must provide the District with proof satisfactory to the District that the above requirements have been met, prior to the commencement of work or use of District facilities. The failure of the District to object to the contents of the certificate or the absence of same will not be deemed a waiver of any and all rights held by the District. Upon request, the Consultant will provide the District with a copy of the Consultant's applicable insurance policies including any endorsements, modifications, or exclusions thereto.

If the Consultant contracts with any others to provider Services pursuant to this Agreement, then the contracts between the Consultant and such other parties must meet all requirements set forth in this Paragraph. The Consultant must deliver to the District adequate proof of insurance for each other party prior to allowing such party to perform services pursuant to this Agreement. The District must be listed as an additional insured on the insurance policies of such other parties by using endorsement CG 2026 or its equivalent.

5. Safeguarding Information: Neither the Consultant nor the District will use or disclose any information concerning the Services pursuant to this Agreement for any purpose which is prohibited by Federal and State statutes and/or regulations.

6. The section dealing with Notices of the Agreement will be deleted and replaced with: Any notices required or permitted to be given pursuant to the terms of this Agreement must be in writing and either personally delivered or sent by nationally recognized overnight carrier to the parties at the following addresses:

To the Consultant:

To the District:

Commack Union Free School District
P.O. Box 150
Commack, New York 11725
Attention: Superintendent of Schools

With a copy to:

Lamb & Barnosky, LLP
534 Broadhollow Road, Suite 210
P.O. Box 9034
Melville, New York 11747
Attention: Eugene R. Barnosky, Esq.

7. Entire Agreement: This Agreement contains the entire agreement of the parties with respect to the subject matter thereof and supersedes any and all other agreements, understandings and representations, written or oral, by and between the parties.

8. Modification: This Agreement may not be changed orally, but only by an agreement in writing signed by the party or parties against whom an enforcement of any waiver, change, modification, extension or discharge is sought. Any waiver of any term, condition or provision of this Agreement will not constitute a waiver of any other term, condition or provision, nor will a waiver of any breach of any term, condition or provision constitute a waiver of any subsequent or succeeding breach.

9. No Assignment: In accordance with the provisions of General Municipal Law § 109, the Consultant is hereby prohibited from assigning, transferring, conveying, subletting or otherwise disposing of this Agreement, or of the Consultant's rights, title, or interest in this agreement, or the Consultant's power to execute this Agreement to any other person or corporation without the previous consent in writing from the District.

10. Third-Party Beneficiaries: There are no third-party beneficiaries of or in this Agreement.

11. Negotiated Agreement: This is a negotiated Agreement. It will not be construed against any party by reason of this Agreement being prepared by that party's attorney. Each party warrants that it/he/she has full power to execute, deliver and perform this Agreement and has taken all actions required by law, organizational documents or otherwise to authorize the execution and delivery of this Agreement.

12. Plan for Security and Protection of Personally Identifiable Information.

A. “District Data” means all information obtained by the Consultant from the District or by the Consultant in connection with the Services provided by the Consultant pursuant to this Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, “District Data” does not include any information made publically available by the District, except PII from student and personnel data which will be considered “District Data” regardless of whether or not it is made public.

B. “Personally Identifiable Information” or “PII” includes, but is not limited to: (i) a person’s name or address or the names or addresses of a student’s parents or other family members; (ii) any personal identifier (e.g., SSN, student number or biometric record); (iii) indirect identifiers (e.g., date of birth, place of birth, or mother’s maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or Consultant reasonably believes knows the identity of the person to whom a record relates.

C. The Consultant represents and warrants that it will comply with all District policies and State, federal and local laws, regulations, rules and requirements related to the confidentiality, security and privacy of District Data.

D. The Consultant represents and warrants that District Data received by the Consultant will be used only to perform Consultant’s obligations pursuant to the Agreement and for no other purpose.

E. The Parties agree that all rights including all intellectual property rights in and to District Data will remain the exclusive property of the District and that the Consultant has a limited, non-exclusive license to use District Data solely to perform

the Services pursuant to the Agreement.

F. If the Consultant has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Consultant acknowledges that for purposes of the Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Consultant agrees to abide by the limitations and requirements imposed on school officials.

G. The Consultant must execute and deliver the Data Privacy Agreement annexed hereto as Exhibit A simultaneously with the execution and delivery of this Rider. The terms of the Data Privacy Agreement are hereby incorporated into this Rider.

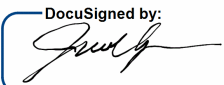
H. All the provisions of this Paragraph will survive the expiration or sooner termination of the Agreement.

13. Execution: The Agreement may be executed in one or more counterparts, all of which will be considered one and the same agreement. The Agreement may be executed by facsimile or PDF signature, each of which will constitute an original for all purposes.

IN WITNESS WHEREOF, the parties hereto have set their respective hands and seals as of the date and year first above written.

COMMACK UNION FREE
SCHOOL DISTRICT

FIVE TOWNS COLLEGE

By: 
1A3F907ADAB2482...
Justin Varughese, President


By: 
Name: Marsha Pollard
Title: Provost

EXHIBIT A
DATA PRIVACY AGREEMENT

**COMMACK UNION FREE SCHOOL DISTRICT
DATA PRIVACY AGREEMENT**

Between

COMMACK UNION FREE SCHOOL DISTRICT

and

This Data Privacy Agreement ("DPA") is by and between the Commack Union Free School District ("the District") and FIVE TOWNS COLLEGE ("the Contractor"), collectively, "the Parties."

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information of District Data, or a breach of the Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** The sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of Personally Identifiable Information by any means, including oral, written or electronic, whether intended or unintended.
4. **District Data:** All information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to the Service Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except Personally Identifiable Information from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.
5. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
6. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, School, or the New York State Education Department.
7. **Eligible Student:** A student who is eighteen years of age or older.
8. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR § 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
9. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
10. **Parent:** A parent, legal guardian or person in parental relation to the Student.

11. Personally Identifiable Information ("PII"): Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

12. Release: Has the same meaning as Disclose.

13. Service Agreement:

The agreement between the District and the Contractor with an effective date of July 1, 2023.

14. Services: The services provided by the Contractor to the District pursuant to the Service Agreement.

15. School: Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

16. Student: Any person attending or seeking to enroll in an Educational Agency.

17. Student Data: Personally Identifiable Information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g. Personally Identifiable Information includes, but is not limited to: (i) a person's name or address or the names or addresses of a Student's parents or other family members; (ii) any personal identifier (e.g., SSN, student number or biometric record); (iii) indirect identifiers (e.g., date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the District community who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or the Contractor reasonably believes know the identity of the person to whom a record relates.

18. Subcontractor: The Contractor's non-employee agents, consultants and/or other persons or entities not employed by the Contractor who are engaged in the provision of Services pursuant to the Service Agreement.

19. Teacher or Principal APPR Data: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to Release pursuant to the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law

In order for the Contractor to provide Services to the District pursuant to the Service Agreement; the Contractor may receive District Data regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. §§ 6501-6506 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. § 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. § 1400 et seq. (34 CFR Part 300); New York Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law and to protect District Data. The Contractor agrees to

maintain the confidentiality and security of District Data in accordance with applicable New York, federal and local laws, rules and regulations.

2. *Authorized Use*

The Contractor has no property or licensing rights or claims of ownership to District Data, and the Contractor must not use District Data for any purpose other than to provide the Services set forth in the Service Agreement. The Contractor agrees that neither the Services provided to the District nor the manner in which the Services are provided by the Contractor will violate applicable New York, federal and local laws, rules and regulations.

If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of this Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Consultant agrees to abide by the limitations and requirements imposed on school officials.

3. *Collection of Data*

The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use the Services) that is necessary to fulfill the Contractor's duties pursuant to the Service Agreement.

4. *Data Security and Privacy Plan*

The Contractor must adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect District Data in a manner that complies with New York, federal and local laws, rules and regulations and the District's policies. Education Law § 2-d requires that the Contractor provide the District with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable State, federal and local data security and privacy requirements. The Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C and is incorporated into this DPA.

5. *The District's Data Security and Privacy Policy*

State law and regulation requires the District to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. The Contractor represents and warrants that it will comply with the District's data security and privacy policy and other applicable policies.

6. *Right of Review and Audit*

Upon request by the District, the Contractor will provide the District with copies of its policies and related procedures that pertain to the protection of PII and District Data. The policies and procedures may be made available in a manner that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required by the District to undergo an audit of Contractor's privacy and security safeguards, measures and controls as they pertain to alignment with the requirements of applicable New York, federal and local laws, rules and regulations, the District policies applicable to the Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at the Contractor's expense, and provide the written audit report to the District. The Contractor may provide the District with a recent industry standard audit report performed by an independent third party on the Contractor's privacy and security practices as an alternative to undergoing an audit. The determination of whether the previously prepared audit report is "recent" will be determined by the District in its sole judgment.

7. *Access to/Disclosure of District Data*

- (a) The Contractor agrees that it will limit the Contractor's internal access to and only Disclose PII to the Contractor's officers, employees and Subcontractors who need to access the PII in order to provide the Services and that the disclosure of PII will be limited to the extent necessary to provide the Services pursuant to the Service Agreement. The Contractor must take all actions necessary to ensure that all its officers, employees and Subcontractors comply with the terms of this DPA.
- (b) The Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to District Data must be contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) The Contractor must examine the data security and privacy measures of its Subcontractors prior to utilizing the Subcontractor to ensure compliance with this DPA. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, the Contractor must: notify the District and prevent the Subcontractor's continued access to District Data; and, as applicable, retrieve all District Data received or stored by Subcontractor and/or ensure that District Data has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, the Contractor must follow the Data Breach reporting requirements set forth herein.
- (d) The Contractor will take full responsibility for the acts and omissions of its officers, employees and Subcontractors.
- (e) The Contractor must not Disclose District Data to any other party (a party other than the Contractor's officers or employees or Subcontractors who does not need access to the District Data to provide the Services pursuant to the Service Agreement) without the prior written consent of the District (if necessary, the District will obtain the required consent(s) from third parties) unless the disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the District of the court order or subpoena in advance of compliance but in any case, provides notice to the District no later than the time the District Data is disclosed, unless such disclosure to the District is expressly prohibited by the statute, court order or subpoena.
- (f) Except as prohibited by law, the Contractor will: (i) immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking District Data; (ii) consult with the District regarding the Contractor's response; (iii) cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and (iv) upon the District's request, provide the District with a copy of the Contractor's response.
- (g) Upon the District's request, the Contractor agrees that it will promptly make any District Data held by the Contractor available to the District.

8. *Training*

The Contractor must ensure that all its officers, employees and Subcontractors who have access to PII have received or will receive training on the federal and State laws governing confidentiality of the data prior to receiving access.

9. *Term and Termination*

This DPA will be effective as of the date the Service Agreement is effective and will terminate on the termination of the Service Agreement. However, the obligations of the parties pursuant to this DPA will survive the expiration of the Service Agreement and will continue until the Contractor and Subcontractors no longer retain PII and no longer retain access to PII.

10. *Data Return and Destruction of Data*

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the District, and the Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the District, unless such retention is expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, expressly requested by the District for purposes of facilitating the transfer of PII to the District or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, the Contractor will transfer PII, in a format agreed to by the Parties to the District.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the District's written election to do so, the Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by the Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, or electronic imaging of hard copies) as well as any and all PII maintained on behalf of the Contractor in a secure data center and/or in cloud-based facilities that remain in the possession of the Contractor or its Subcontractors, the Contractor will ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) The Contractor will provide the District with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that the Contractor and/or its Subcontractors continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), the Contractor agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

11. *Commercial or Marketing Use Prohibition*

Contractor agrees that it will not sell PII or use or Disclose PII for a Commercial or Marketing Purpose.

12. *Encryption*

The Contractor will use industry standard security measures including Encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must Encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

13. *Storage*

Contractor must store all District Data within the United States of America.

14. *Breach*

- a. The Contractor must promptly notify the District of any Breach of PII in the most expedient way possible and without unreasonable delay and in no event more than seven calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing and by email (if email address is provided) and personal delivery or nationally recognized overnight carrier. Notifications must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the District. Violations of the requirement to notify the District are subject to civil penalty(ies) pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law §2-d may subject the Contractor to additional penalties.
- b. Notifications required to be made to the District pursuant to this paragraph must be sent to the following people at the following addresses:

Dr. Jordan F. Cox
Superintendent of Schools
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: jcox@commack.k12.ny.us

Mr. Timothy Russo
Assistant Superintendent for Curriculum, Instruction & Assessment
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: trusso@commack.k12.ny.us

15. *Cooperation with Investigations*

Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' officers, employees or Subcontractors, as related to such investigations, will be the sole responsibility of the Contractor if the Breach is attributable to Contractor or its Subcontractors.

16. *Notification to Individuals*

Where a Breach of PII occurs that is attributable to Contractor, Contractor will pay for or promptly reimburse the District for the full cost of the District's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. *Parent and Eligible Student Access*

Education Law § 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the District. To the extent Student Data is held by the Contractor pursuant to the Service Agreement, the Contractor must respond within 20 calendar days to the District's requests for access to Student Data so the District can facilitate review by a

Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by the Contractor pursuant to the Service Agreement, the Contractor must promptly notify the District and refer the Parent or Eligible Student to the District.

2. *Bill of Rights for Data Privacy and Security*

As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are annexed hereto as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. The Contractor must complete and sign Exhibits A and B. Pursuant to Education Law § 2-d, the District is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. *Priority of Agreements and Precedence*

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA will govern and prevail, will survive the termination of the Service Agreement in the manner set forth herein, and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. *Execution*

This DPA may be executed in one or more counterparts, all of which will be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto will be and constitute an original signature, as if all parties had executed a single original document.

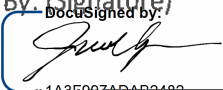

Commack Union Free School District	
By: (Signature)  <small>DocuSigned by: 1A3F997ADAB2482...</small>	By: (Signature) 
Justin Varughese	(Printed Name) Marsha Pollard
President, Board of Education	(Title) Provost
Date: 9/8/2023	Date: 9/28/23

EXHIBIT A - Education Law § 2-d Parents' Bill of Rights for Data Privacy and Security

COMMACK UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY --

Summary of Rights and Information for Parents and Students

The legislature and governor passed a group of bills that adjusted the Regents Education Reform Agenda. These bills are known collectively as the "Common Core Implementation Reform Act." One of the key components of this act (Chapter 56, Part AA, Subpart L, of the laws of 2014) directs the Commissioner of Education to appoint a Chief Privacy Officer (CPO). A major function of this new position is to work with school districts and parents to develop elements for a parents' bill of rights to help ensure that student data is private and secure. The State Education Department (SED) and the CPO must also recommend regulations to establish standards for data security and privacy policies that will be implemented statewide.

SED has issued a preliminary Parents' Bill of Rights for Data Privacy and Security. The Commack Union Free School District is issuing this summary of parents' rights under the new law. While some additional elements will be developed in conjunction with the CPO, districts, parents and the Board of Regents, this summary sets forth the key rights and information that parents should be aware of in regards to ensuring the privacy and security of their student's educational data.

The Commack Union Free School District is committed to ensuring student privacy and recognizes that parents, legal guardians, and persons with a parental relationship to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. To this end, the District is providing the following Parent's Bill of Rights for Data Privacy and Security:

1. A student's personally identifiable information cannot be sold or released for any 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, 89 Washington Avenue, New York 12234; and
5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. Complaints should be addressed to Mr. Timothy Russo, Asst. Supt. for Curriculum, Instruction & Assessment, PO Box 150, Commack, New York

11725, Phone: (631) 912-2009, Email: trusso@commack.k12.ny.us or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

If the Commack Union Free School District enters into a third-party contract in which the service provider receives student data or teacher or principal data in order to provide a needed service for the District, supplemental information shall be developed and provided to parents that states:

- 6. The exclusive purposes for which the student data or teacher or principal data will be used;
- 7. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- 8. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
- 9. 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; and
- 10. Where the student data or teacher or principal data will be stored and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The CPO as appointed by the Commissioner must secure input from parents and other education and expert stakeholders to develop additional elements for the Parents' Bill of Rights for Data Privacy and Security. The Commissioner of Education will also be promulgating regulations with a comment period for parents and other members of the public to submit comments and suggestions to the CPO.

In the meantime, you can access additional information and a question and answer document issued by SED as a preliminary Parents' Bill of Rights for Data Privacy and Security.

If you have any further questions or concerns at this time, please contact Dr. Jordan F. Cox, Superintendent, Commack UFSD, PO Box 150, Commack, New York 11725 or Mr. Timothy Russo at trusso@commack.k12.ny.us (update email).

By: (Signature)	<i>Marsha Pollard</i>
(Printed Name)	Marsha Pollard
(Title)	Provost
Date:	8/28/23

EXHIBIT B: BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and 8 NYCRR § 121.3, the District is required to post information to its website about its contracts with third-party contractors ("Service Agreements") that will receive Personally Identifiable Information ("PII") from Student Data or Teacher or Principal APPR Data.

Term of Service Agreement	Agreement Start Date: JULY 1, 2023 Agreement End Date: JUNE 30, 2024
Description of the purpose(s) for which Contractor will receive/ access / use PII	<p>PII received by the Contractor will be received, accessed and used only to perform the Contractor's Services pursuant to the Service Agreement with the District.</p> <p>List Purposes: A) FIVE TOWNS COLLEGE - STUDENTS WILL RECEIVE COLLEGE CREDIT VIA A DUAL ENROLLMENT AGREEMENT B) ENROLLMENT REPORTING TO THE NATIONAL STUDENT CLEARINGHOUSE</p>
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> Teacher or Principal APPR Data</p>
Subcontractor Written Agreement Requirement	<p>The Contractor will only share PII with entities or persons authorized by the Service Agreement. The Contractor will not utilize Subcontractors without written contracts that require the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Service Agreement.</p> <p>Check applicable option.</p> <p><input checked="" type="checkbox"/> Contractor will not utilize Subcontractors.</p> <p><input type="checkbox"/> Contractor will utilize Subcontractors.</p>
Data Transition and Secure Destruction	<p>Upon expiration or termination of the Service Agreement, the Contractor will, as directed by the District in writing:</p> <ul style="list-style-type: none"> • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data by taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means.
Challenges to Data Accuracy	Parents, students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed

	necessary, the District will notify the Contractor. The Contractor agrees to facilitate such corrections within 21 calendar days of receiving the District's written request.
Secure Storage and Data Security	<p>The Contractor will store and process District Data in compliance with § 2-d(5) and applicable regulations of the Commissioner of Education, as the same may be amended from time to time, and in accordance with commercial best practices, including appropriate administrative, physical and technical safeguards, to secure district Data from unauthorized access, disclosure, alteration and use. The Consultant will use legally-required, industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing services pursuant to the Service Agreement. The Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.</p> <p>Please describe where PII will be stored and the security protections taken to ensure PII will be protected and data security and privacy risks mitigated in a manner that does not compromise the security of the data:</p> <p>(a) Storage of Electronic Data (check all that apply):</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.<input type="checkbox"/> Using Contractor owned and hosted solution<input type="checkbox"/> Other: <p>(b) Storage of Non-Electronic Data: <i>WILL BE KEPT IN LOCKED FILE CABINETS IN ADMISSIONS AND/OR THE REGISTRAR OFFICE</i></p> <p>(c) Personnel/Workforce Security Measures: <i>WILL BE KEPT IN LOCKED FILE CABINETS WITH THE REGISTRAR</i></p> <p>(d) Account Management and Access Control: <i>USING A CLOUD OR INFRASTRUCTURE (EX: CAMPUS CAFE OR CANVAS)</i></p> <p>(e) Physical Security Measures: <i>STORAGE IN LOCKED FILE CABINETS</i></p> <p>(f) Other Security Measures: <i>ON-CAMPUS FIREWALLS AND ANTI-VIRUS FOR ALL WORKSTATIONS</i></p>
Encryption	Data will be encrypted while in motion and at rest.

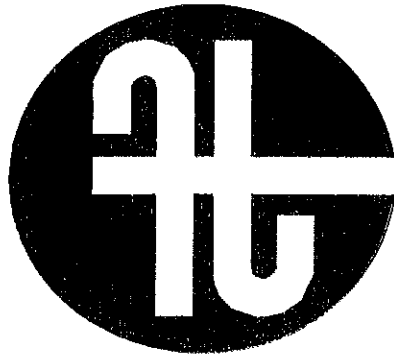
By: (Signature)	<i>Marsha Pollard</i>
(Printed Name)	Marsha Pollard
(Title)	Provost
Date:	8/28/23

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN AS A LINK:

https://www.ftc.edu/wp-content/uploads/2023/03/DATA-SECURITY-POLICY-2.ED_.2023.pdf



FIVE TOWNS COLLEGE

DATA SECURITY POLICY & PROCEDURES PROGRAM

The Information Technology (IT) Department

I. Introduction

The protection of sensitive College data and information is of paramount importance. The Information Technology (IT) Department is dedicated to preventing the unauthorized access or disclosure of this information. To assure this, the IT Department has implemented several measures to minimize the risk of unauthorized access. Accordingly, and in response to federal, state and other regulations, including institutional policies, the College is determined to effectuate policies and procedures that safeguard the receipt, collection, storage and then, disposal of this data.

II. Role of IT Department and Individual Designated to Coordinate the Information Security Program

Five Towns College IT Department is the institution's purveyor of both hardware and software and procures appropriate technology for the College. It is thus charged with the responsibility to manage and implement the data security policies and procedures program with the objective to ensure the protection of important and sensitive institutional data and information. Further, the IT Department complies with relevant federal, state, and other regulations and institutional policies. To this end, the institution has designated the Head of the IT Department to coordinate the data security program.

III. Relevant Laws and Regulations

As a recipient of Title IV funds, Five Towns College is classified as a financial institution under the Gramm-Leach-Bliley Act (GLBA, 2002), which is also known as the Financial Modernization Act of 1999. It is a federal law enacted to control the ways that financial institutions deal with the private information of individuals and, thus, there must be certain safeguards in place. Included in these are (1) the development, implementation, and maintenance of a documented data security program; and (2) the designation of an employee to coordinate the program.

In furtherance of this compliance, the College has developed these policies, trained staff, and has reviewed its technology, including built-in systems safeguards as well as identifying areas to strengthen, if deemed necessary.

Here are the three elements required by 16 C. F. R. 314.4(b):

In order to develop, implement, and maintain your information security program, you shall:

- (a) **Designate an employee** or employees to coordinate your information security program.
- (b) **Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.** At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
 - (1) Employee training and management;
 - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
 - (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
- (c) **Design and implement information safeguards to control the risks** you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- (d) Oversee service providers, by:
 - (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
 - (2) Requiring your service providers by contract to implement and maintain such safeguards.
- (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program. (Emphasis supplied) (16 C. F. R. 314.4(b)).

IV. Institutional Initiatives

To effectuate an improvement in procedures and be compliant, several institutional offices, including Admissions, Financial Aid and Registrar have implemented new processes to protect incoming data and design a paper flow that is primarily digital but is protected with appropriate safeguards. Part of this is demonstrated by changed procedures in the Admissions Office with an online application process with secure software in place as well as captcha software. Also, the Financial Aid Department has implemented a secure portal to upload important and sensitive documents with proper authentication and password protection. Further, the Registrar's Office has both interactive and PDF versions of forms for important data requests.

V. Data Protection and Account Security Measures

The IT Department has implemented several data protection and account security measures. These security measures include but are not limited to the following:

- Password Policy requires passwords to be changed every six months and follow certain criteria.
- A firewall is in place to block unauthorized traffic and networking hardware is all password protected.
- Network accounts and permissions are implemented.
- Microsoft Active Directory controls Network Access.
- Public websites protected by secure socket layers.
- No access to computers/shared storage only to permitted staff.
- Computers lock after 10 minutes of inactivity.
- Anti-virus is installed on all computers.
- Users with personal computers are limited to Wi-Fi service which is restricted to outbound traffic to the Internet.
- Data is remotely backed up with security in place.
- All applications are password protected.
- Accounts and access for staff/faculty are verified with supervisors.
- Institutional policy not to email social security number or other personally identifiable information.

VI. Institutional Information Risk Assessment and Testing Schedule

Pursuant to the regulations stated above, the institution must perform a risk assessment that addresses the three areas noted above. In addition to account security measures described above, the institution conducts information technology risk assessment. This assessment is on demand, and a monthly/regular schedule is available upon request from the Head of the IT Department.

VII. Institutional Documentation of Information Risk Assessment/Testing Schedule Test and Results

To evidence that the stated risk assessment is conducted and that the testing schedule tests and results are recorded, the institution has developed a plan to record this information. Currently, this is performed monthly and the documentation is available upon written request as appropriate or required from the Head of the IT Department.

VIII. Information Security Policy and Procedures Program Schedule and Contact Information Available on Consumer Information and Compliance Website

For all questions or concerns related to the FTC IT Data Security Policies and Procedures Program and schedule, please contact the Head of the IT Department, Craig Healy. He actively oversees this process and can be contacted at support@ftc.edu.

IX. Communications: Preparedness to Respond Immediately and Appropriately in the Event of Breach

In the event of a breach of these security measures, an internal investigation would be initiated at once and a diagnostic plan would follow. A communications plan has been established among the institution's executive team that includes immediate notification from the IT Department to the Public Safety Office, the Vice President of Finance and Administration and President. Once the source or area of the institution's data involved is determined, all heads of those and other administrative units are notified. The College's Administrative Council has met, discussed, reviewed, and is involved in all notifications that will be sent to the institution's constituents in this event, as well as to the local precinct and public, depending on the situation.

X. Data Security Policies and Procedures Program Related to Third Parties Under Articulation and Dual Enrollment Agreements

The College has several Articulation and Dual Enrollment Agreements with area high schools and/or community colleges. Under those agreements, any related data provided i.e., personally identifiable information as defined by New York Education Law Section 2-d, and/or the Family Educational Rights and Privacy Act (FERPA) is afforded the same protections and is managed under the terms and provisions of the College's Data Security Policies and Procedures Program detailed here and in compliance with state and federal law. Any requests to provide its institutional data security and privacy plan are herein contained and all third parties hereby have acknowledged that they have received actual and/or constructive notice of this as part and parcel of the underlying Articulation and/or Dual Enrollment Agreement(s).

Further, and in conformance with this, the College understands and acknowledges that it has in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it: (1) limits internal access to education records to those individuals that are determined to have legitimate educational interests; (2) does not use the education records for any purposes other than those explicitly authorized in those Agreements; (3) maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and (4) has adopted this institutional Data Security Policy and Procedures Program in compliance with the above that addresses confidentiality, data security and privacy standards and it is available at ftc.edu.