

DUAL ENROLLMENT AGREEMENT
by and between
Hauppauge Union Free School District and Five Towns College

Effective September 1, 2024 to June 30, 2027

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

WHEREAS, both the District 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 the District 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 the College, and

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

- To provide an opportunity for the District 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 the District 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, 2024, and shall remain in effect until June 30, 2027.

The College shall be responsible for:

- Providing of the designated course overviews to the District to ensure these courses offered at the College are taught at the high school;
- Providing a tuition scholarship of at least 25% or more for students who pursue post-secondary study at the College;
- Identify opportunities for the District Students to participate in the activities of the College;
- Inviting students to tour the campus; and
- Notifying the District School of any changes in the agreement.

The District School shall be responsible for:

- Teaching the designated College course as defined by the College's Course Overview and The District curriculum;
- Providing to the College the instructor's CV, NYSED license certifications and college transcripts.
- Planning the schedule of student assignments to include all of the coursework, assessments, and outcomes agreed by and with the District.

In order for a District student to receive credits from the College, the student must:

- Be in the Junior or Senior year to receive College credit;
- Register for the course as instructed by the District teacher and pay a \$50 administrative fee for each course directly to the College;
- Successfully complete the College's curricula as detailed by this agreement and offered by the District 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 the District 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.

Plan for Security and Protection of Personally Identifiable Information:

- A. "District Data" means all information obtained by the College from the District or by the College 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 publicly available by the

District, except 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 addresses of a student's parents or other family members (ii) any personal identifies (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 College reasonably believes knows the identity of the person to whom a record relates.
 - C. The College 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 College represents and warrants that District Data received by the College will be used to perform College's obligations pursuant to this Agreement and for no other purpose.
 - E. The College 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 services provided by the College pursuant to this Agreement) that is necessary to fulfill the College's duties pursuant to this Agreement.
 - F. 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 College has a limited, non-exclusive license to use District Data solely to perform the Services pursuant to this Agreement.
 - G. The College has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the College acknowledges that for the 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 College agrees to abide by the limitations and requirements imposed on school officials.
 - H. The College must execute and deliver the Data Privacy Agreement annexed hereto as Exhibit B simultaneously with the execution and delivery of this Agreement.
 - I. Paragraphs A-H under the heading, " Plan for Security protection of Personally Identifiable Information" will serve to expiration or sooner termination of this Agreement.
- J. Furthermore, Five Towns College includes and incorporates by reference its Data Security Policy and Procedures Program with 2024 updates which is consistent with the spirit and

requirements set forth herein: The link is attached here: https://www.ftc.edu/wp-content/uploads/2024/06/DATA-SECURITY-POLICY-2.ED_2024.updated.pdf

In particular, under section X, the policy states, in part,

“ . . . 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. . . ”

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 mailed or emailed to:

Dr. Tim McCarthy
Assistant Superintendent for Curriculum, Instruction & Technology
Hauppauge Union Free School District
495 Hoffman Lane
Hauppauge, New York, 11788
mccarthy@hauppauge.k12.ny.us


and


Dr. Marsha Pollard
Provost
Five Towns College
305 North Service Road
Dix Hills, New York, 11746
Marsha.pollard@ftc.edu


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. This Agreement may be terminated at any time, by the District for convenience upon 30 days calendar days’ written notice to the College.


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 constitute a waiver of any other term, condition or provision, nor will a waiver of any breach of any term, condition constitute a waiver of any subsequent or succeeding breach.

IN WITNESS WHEREOF, the parties have executed this Agreement.

By: 
Sharon Ryba-Pertz
Interactive Media Art Division Chair, Five Towns College
8/20/24
Date

By: 
Dr. David Krasner
Theatre Arts Division Chair, Five Towns College
7/29/24
Date

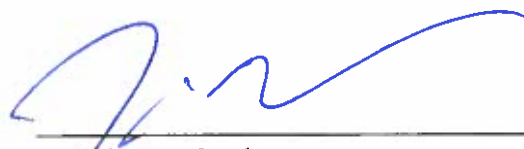
By: 
Holli Haerr
Mass Communication Division Chair, Five Towns College
7/31/24
Date

By: 
Dr. Marsha Pollard
Provost, Five Towns College
10/11/24
Date

By: 

David Barshay
President, Board of Education
Hauppauge Union Free School District

10/15/24
Date

By: 

Dr. Tim McCarthy
Assistant Superintendent for Curriculum, Instruction & Technology
Hauppauge Union Free School District

10/9/24
Date

FIVE TOWNS COLLEGE
Dual Enrollment Components

The following Five Towns College courses have been approved for credit in a dual enrollment agreement with Hauppauge Union Free School District. Final approval was based upon discussion and agreement with Chairpersons of the College and the Administration of The Hauppauge Union Free School District.

SCHEDULE A

Hauppauge Union Free School District	Five Towns College Course	Credits
0725B- Television Broadcast	VID131- Introductory Production: TV Workshop	3
0712 - Advanced Computer Graphics	MAC280- Digital Media Art: Design	3
0817- Advanced Acting Ensemble	THR124 – Acting 2	3
0821A/B Musical Theatre	THR107- Musical Theatre	3

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

Between

HAUPPAUGE UNION FREE SCHOOL DISTRICT

and

Five Towns College

This Data Privacy Agreement ("DPA") is by and between the Hauppauge 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 Dual Enrollment Agreement between the District and the Contractor with an effective date of September 1, 2024.

14. Services: The services provided by the Contractor to the District and its students 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 Contractor 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. Donald B. Murphy
Superintendent of Schools
Hauppauge Union Free School District
495 Hoffman Lane
Hauppauge, NY 11788-2836
Email: murphydo@hauppauge.k12.ny.us

Dr. Tim McCarthy
Data Protection Officer
Hauppauge Union Free School District
495 Hoffman Lane
Hauppauge, NY 11788-2836
Email: mccarthyt@hauppauge.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.


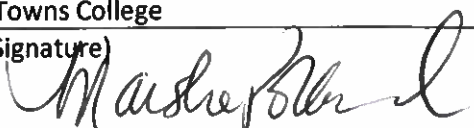
ARTICLE IV: MISCELLANEOUS

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.

Hauppauge Union Free School District	Five Towns College
By: (Signature) 	By: (Signature) 
David Barshay	Dr. Marsha Pollard
President, Board of Education	Provost
Date: 10/15/24	Date: 10/1/24

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

HAUPPAUGE UNION FREE SCHOOL DISTRICT

**PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY
Summary of Rights and Information for Parents and Students**

The Hauppauge Union Free School District is committed to ensuring the privacy of student personally identifiable information and recognizes that parents (including legal guardians or persons in parental relationships) and eligible students (students 18 years of age and older) are entitled to certain rights with regard to a student's personally identifiable information. 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 ("PII") cannot be sold or released for any commercial purposes. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR § 99.3 for a more complete definition.
2. Parents and/or eligible students have the right to inspect and review the complete contents of the student's education records stored or maintained by the District. This right may not apply to parents of an eligible student.
3. State and federal laws such as New York Education Law § 2-d, the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA, the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and the Individuals with Disabilities Education Act protect the confidentiality of a student's PII.
4. 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.
5. A complete list of all student data elements collected by the State is available for public review at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. Parents have the right to have complaints about possible breaches and unauthorized disclosures of PII addressed.

- a. Complaints should be submitted to the District at: Dr. Tim McCarthy, District Data Protection Officer, Hauppauge UFSD, P.O. Box 6006, Hauppauge, New York 11788, mccarthyt@hauppauge.k12.ny.us, 631-761-8202.
 - b. Complaints may also be submitted to the New York State Education Department at: www.nysed.gov/data-privacy-security/report-improper-disclosure or by contacting the State's Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, privacy@nysed.gov, 518-474-0937.
7. District contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements and will include supplemental information that provides:
- a. The exclusive purposes for which student data or teacher or principal data will be used;
 - b. How the third party contractor will ensure that the subcontractors, persons or entities that the vendor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
 - c. When the agreement expires and what happens to student data or teacher or principal data upon expiration of the agreement;
 - d. 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
 - e. 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 how such data will be encrypted.
8. Parents and/or eligible students have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
9. District workers who handle PII will receive annual training on applicable federal and State laws, regulations, policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

Five Towns College	
By: (Signature)	<i>Marsha Pollard</i>
Dr. Marsha Pollard	
Provost	
Date:	<i>10/1/24</i>

EXHIBIT B: BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

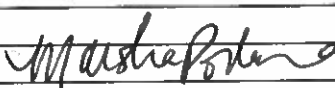
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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.

Five Towns College	
Term of Service Agreement	<p>Agreement Start Date: September 1, 2024 Agreement End Date: June 30, 2027</p>
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:</p> <ol style="list-style-type: none"> 1. High School students that are enrolled in specific courses outlined in the dual enrollment agreement will receive college credit. 2. Enrollment will be reported to the National Clearing House
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>

	<input type="checkbox"/> Contractor will utilize Subcontractors.
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	<p>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.</p>
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 Contractor 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:</p>

	<p>(c) Personnel/Workforce Security Measures:</p> <ol style="list-style-type: none"> 1. Kept in locked file cabinets. 2. Password changes every 6 months <p>(d) Account Management and Access Control:</p> <ol style="list-style-type: none"> 1. Utilize Microsoft Active Directory. <p>(e) Physical Security Measures:</p> <ol style="list-style-type: none"> 1. Storage in locked file cabinets <p>(f) Other Security Measures:</p> <ol style="list-style-type: none"> 1. On campus firewalls and anti-virus software.
Encryption	Data will be encrypted while in motion and at rest.

Five Towns College	
By: (Signature)	
Dr. Marsha Pollard	
Provost	
Date:	10/1/24

In response, Five Towns College is providing its Data Security Policies & Procedures Program hereto that materially addresses alignment with the requirements of the NIST Cybersecurity Framework and incorporates and refers to all of the relevant federal and state regulations including FERPA, Education Law Section 2-d and others. The link to the document is:

https://www.ftc.edu/wp-content/uploads/2024/06/DATA-SECURITY-POLICY-2.ED_2024.updated.pdf

EXHIBIT C - CONTRACTOR’S DATA PRIVACY AND SECURITY PLAN

The Hauppauge Union Free School District is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan pursuant to Education Law § 2-d and Section 121.6 of the Commissioner’s Regulations. The Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. The terms of the plan cannot conflict with any other terms of or Exhibits to the Data Privacy Agreement to which this Exhibit C is attached. **While this plan is not required to be posted to the District’s website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems. DO NOT LIMIT RESPONSES TO THE SPACES PROVIDED.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
3	Specify how your officers, employees and Subcontractors who have access to PII pursuant to the Service Agreement will receive training on the federal and State laws that govern the confidentiality of PII.	
4	Outline the processes that ensure that your officers, employees and Subcontractors are bound by written agreement to the requirements of the Service Agreement, at a minimum.	
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the District.	

6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the District.	
8	Outline how your data security and privacy program/practices align with the District's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	YOU MAY USE TEMPLATE BELOW

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support	

	operational risk decisions.	
PROJECT (PR)	<p>Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	
	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	
	<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	
	<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p>	
	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	

	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	
<p>DETECT (DE)</p>	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	
<p>RESPOND (RS)</p>	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	
<p>RECOVER (RC)</p>	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	
	<p>Communications (RC.CO): Restoration activities are coordinated with internal</p>	

and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).



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 Qualified Individual 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 Director of the IT Department as its qualified individual responsible for overseeing, implementing and enforcing the FTC information 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.

Following its enactment, the GLBA has been modified from time to time. In 2021, provisions considered as the Standards for Safeguarding Customer Information were modified and the effective date was extended to June 9, 2023. The College adheres to the requirements of this regulation. Provisions of 16 C.F.R. section 314.3 and 16 C.F.R. section 314.4 and its provisions are set forth below:

§314.3 Standards for safeguarding customer information.

(a) **Information security program.** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) **Objectives.** The objectives of section 501(b) of the Act, and of this part, are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70307, Dec. 9, 2021]

314.4 Elements.

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

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

- (1) Retain responsibility for compliance with this part;
- (2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and
- (3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

(b) Base your information security program on a risk assessment that identifies 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 assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(2) You shall periodically perform additional risk assessments that reexamine the 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 reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement safeguards to control the risks you identify through risk assessment, including by:

(1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;

(4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

(5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6)

(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

(d)

(1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

(i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) 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;

(2) Requiring your service providers by contract to implement and maintain such safeguards; and

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:

(1) The goals of the incident response plan;

(2) The internal processes for responding to a security event;

(3) The definition of clear roles, responsibilities, and levels of decision-making authority;

- (4) External and internal communications and information sharing;
- (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
- (6) Documentation and reporting regarding security events and related incident response activities; and
- (7) The evaluation and revision as necessary of the incident response plan following a security event.

(i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

- (1) The overall status of the information security program and your compliance with this part; and
- (2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

(j) Notify the Federal Trade Commission about notification events in accordance with paragraphs (j)(1) and (2) of this section.

(1) **Notification requirement.** Upon discovery of a notification event as described in paragraph (j)(2) of this section, if the notification event involves the information of at least 500 consumers, you must notify the Federal Trade Commission as soon as possible, and no later than 30 days after discovery of the event. The notice shall be made electronically on a form to be located on the FTC's website, <https://www.ftc.gov>. The notice shall include the following:

- (i) The name and contact information of the reporting financial institution;
- (ii) A description of the types of information that were involved in the notification event;
- (iii) If the information is possible to determine, the date or date range of the notification event;
- (iv) The number of consumers affected or potentially affected by the notification event;
- (v) A general description of the notification event; and
- (vi) Whether any law enforcement official has provided you with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal

Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

(2) *Notification event treated as discovered.* A notification event shall be treated as discovered as of the first day on which such event is known to you. You shall be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent. [86 FR 70307, Dec. 9, 2021, as amended at 88 FR 77508, Nov. 13, 2023]

§314.6 Exceptions.

Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers. [8 FR 70308, Dec. 9, 2021]

IV. Institutional Initiatives

To effectuate continuing processes and procedures that align with the relevant regulations, FTC's administrative offices, including Admissions, Financial Aid, Registrar, Bursar, and Information Technology (IT) have implemented new processes and software to protect incoming data and design a system that is primarily digital and is protected with appropriate safeguards. This is demonstrated, in part, by changed procedures in the Admissions Office that include an online application process with secure software, and an updated Student Information System (SIS) as well as security software, i.e., reCAPTCHA for supplementary submissions and documents, if needed, as well as the use of an integrated student portal.

The Financial Aid Department has implemented a secure portal to upload important and sensitive documents with proper authentication and password protection. The Registrar's Office uses all safeguards available through the SIS and the institution's Learning Management System (LMS), Canvas, as well. It has also implemented the use of both interactive and PDF versions of forms for important data requests. All of these institutional processes and procedures are secured by the upgraded firewall that ensures current state of the industry technology to alleviate risks to the information systems and the protection of data.

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.
- An updated, state of the art Fortinet firewall blocks unauthorized traffic and ensures that networking hardware is all password protected, in addition to providing backend data and assessment on all attempted and unauthorized access.
- 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 performs risk assessment that addresses the areas noted above. In addition to account security measures described, the institution conducts information technology risk assessment. This assessment is on demand, and also a more frequent data report is reviewed in addition to monthly risk assessment. An annual Risk Assessment Report is conducted by the Qualified Individual and available upon request to authorized parties and supplemented by firewall reports.

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 if required from the qualified individual or the Director 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 qualified individual/Director 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 and in compliance with the notification requirements under the statute. The qualified individual reviews all processes and systems and provides the institution with updated recommendations, including the recommendation to install and implement new updated firewall.

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 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 incorporated into 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 standards for safeguarding consumer information, protections and internal controls to ensure compliance with applicable laws and regulations, and that it is responsible for complying with state/federal 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.



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 Qualified Individual 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 Director of the IT Department as its qualified individual responsible for overseeing, implementing and enforcing the FTC information 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.

Following its enactment, the GLBA has been modified from time to time. In 2021, provisions considered as the Standards for Safeguarding Customer Information were modified and the effective date was extended to June 9, 2023. The College adheres to the requirements of this regulation. Provisions of 16 C.F.R. section 314.3 and 16 C.F.R. section 314.4 and its provisions are set forth below:

§314.3 Standards for safeguarding customer information.

(a) **Information security program.** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) **Objectives.** The objectives of section 501(b) of the Act, and of this part, are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70307, Dec. 9, 2021]

314.4 Elements.

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

(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

- (1) Retain responsibility for compliance with this part;
- (2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and
- (3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

(b) Base your information security program on a risk assessment that identifies 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 assesses the sufficiency of any safeguards in place to control these risks.

(1) The risk assessment shall be written and shall include:

(i) Criteria for the evaluation and categorization of identified security risks or threats you face;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

(2) You shall periodically perform additional risk assessments that reexamine the 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 reassess the sufficiency of any safeguards in place to control these risks.

(c) Design and implement safeguards to control the risks you identify through risk assessment, including by:

(1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

(ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;

(2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

(3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;

(4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

(5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6)

(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

(d)

(1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

(i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) 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;

(2) Requiring your service providers by contract to implement and maintain such safeguards; and

(3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

(g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:

(1) The goals of the incident response plan;

(2) The internal processes for responding to a security event;

(3) The definition of clear roles, responsibilities, and levels of decision-making authority;

(4) External and internal communications and information sharing;

(5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(6) Documentation and reporting regarding security events and related incident response activities; and

(7) The evaluation and revision as necessary of the incident response plan following a security event.

(i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

(1) The overall status of the information security program and your compliance with this part; and

(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

(j) Notify the Federal Trade Commission about notification events in accordance with paragraphs (j)(1) and (2) of this section.

(1) **Notification requirement.** Upon discovery of a notification event as described in paragraph (j)(2) of this section, if the notification event involves the information of at least 500 consumers, you must notify the Federal Trade Commission as soon as possible, and no later than 30 days after discovery of the event. The notice shall be made electronically on a form to be located on the FTC's website, <https://www.ftc.gov>. The notice shall include the following:

(i) The name and contact information of the reporting financial institution;

(ii) A description of the types of information that were involved in the notification event;

(iii) If the information is possible to determine, the date or date range of the notification event;

(iv) The number of consumers affected or potentially affected by the notification event;

(v) A general description of the notification event; and

(vi) Whether any law enforcement official has provided you with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal

Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.

(2) *Notification event treated as discovered.* A notification event shall be treated as discovered as of the first day on which such event is known to you. You shall be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent. [86 FR 70307, Dec. 9, 2021, as amended at 88 FR 77508, Nov. 13, 2023]

§314.6 Exceptions.

Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers. [8 FR 70308, Dec. 9, 2021]

IV. Institutional Initiatives

To effectuate continuing processes and procedures that align with the relevant regulations, FTC's administrative offices, including Admissions, Financial Aid, Registrar, Bursar, and Information Technology (IT) have implemented new processes and software to protect incoming data and design a system that is primarily digital and is protected with appropriate safeguards. This is demonstrated, in part, by changed procedures in the Admissions Office that include an online application process with secure software, and an updated Student Information System (SIS) as well as security software, i.e., reCAPTCHA for supplementary submissions and documents, if needed, as well as the use of an integrated student portal.

The Financial Aid Department has implemented a secure portal to upload important and sensitive documents with proper authentication and password protection. The Registrar's Office uses all safeguards available through the SIS and the institution's Learning Management System (LMS), Canvas, as well. It has also implemented the use of both interactive and PDF versions of forms for important data requests. All of these institutional processes and procedures are secured by the upgraded firewall that ensures current state of the industry technology to alleviate risks to the information systems and the protection of data.

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.
- An updated, state of the art Fortinet firewall blocks unauthorized traffic and ensures that networking hardware is all password protected, in addition to providing backend data and assessment on all attempted and unauthorized access.
- 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 performs risk assessment that addresses the areas noted above. In addition to account security measures described, the institution conducts information technology risk assessment. This assessment is on demand, and also a more frequent data report is reviewed in addition to monthly risk assessment. An annual Risk Assessment Report is conducted by the Qualified Individual and available upon request to authorized parties and supplemented by firewall reports.

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 if required from the qualified individual or the Director 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 qualified individual/Director 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 and in compliance with the notification requirements under the statute. The qualified individual reviews all processes and systems and provides the institution with updated recommendations, including the recommendation to install and implement new updated firewall.

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 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 incorporated into 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 standards for safeguarding consumer information, protections and internal controls to ensure compliance with applicable laws and regulations, and that it is responsible for complying with state/federal 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.