FIVE TOWNS COLLEGE

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

**DUAL ENROLLMENT AGREEMENT**
**by and between**
**District and Five Towns College**

Effective September 1, 2023 to June 30, 2024

*WHEREAS*, a dual enrollment agreement (hereinafter "Agreement") by and between Harborfields Central School District ("District") and Five Towns College (hereinafter the College) that further enhances the education opportunities available for their students is beneficial; and

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

- To provide an opportunity for 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 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, 2023, and shall remain in effect until June 30, 2024.

The College shall be responsible for:

- Providing the designated course overviews to District to ensure these courses offered at the College are taught at the high school;
- Providing scholarship funding for students who pursue post-secondary study at the College;
- Identifying opportunities for District Students to participate in the activities of the College; and
- Inviting students to tour the campus;

District shall be responsible for:

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

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

- Play advanced NYSSMA music selections to receive College credit;
- Be in the Junior or Senior year to receive College credit;
- Register for the course as instructed by the District coordinator and pay a $50 administrative fee directly to the College;
- Successfully complete the College's curricula as detailed by this Agreement and offered by District 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 Exhibit A, a copy of which is annexed hereto and made a part of hereof.

Dropping a course for College Credit is a formal procedure with specific formal paperwork that includes the signature of the student, parent and the District coordinator. There is no refund for dropping a course.

Both District and the College shall endeavor to publicize this Agreement internally to potential students, so that these students and their families will become aware of the opportunities available to them.

The College agrees to defend, indemnify, and hold harmless the District, its officers, trustees, agents, and employees, from any and all suits, claims, losses, damages, or injuries to persons or property, resulting from, arising out of, or in consequence of, any action or cause of action in connection with the actions or omissions of the College, its directors, officers, trustees, agents, students, and/or employees.

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.

The College shall perform all services under this Agreement in accordance with all applicable Federal, State and local laws, rules, and regulations, as well as the established policy guidance from the New York State Education Department. The College shall execute the Education Law 2-d Rider set forth at Exhibit "B", a copy of which is attached. Furthermore, the College hereby incorporates its FTC Data Security Policies and Procedures Program which is available at: https://www.ftc.edu/wp-content/uploads/2023/03/DATA-SECURITY-POLICY-2.ED_.2023.pdf

Either party may terminate this Agreement by written notification of thirty (30) days to the other party.

All notices, consents, demands, requests, approvals and other communications that are required or may be given pursuant to the Agreement shall be in writing and shall be deemed to have been duly given if personally delivered (including overnight courier service) or mailed certified first class mail, postage prepaid:

If to College:
Five Towns College
305 North Service Road,
Dix Hills, NY 11746
Provost, Five Towns College

If to the District:
Harborfields Central School District
2 Oldfield Road
Greenlawn,
New York
11740-1200

*IN WITNESS WHEREOF*, the parties have executed this Agreement.

By: Marsha Pollard

Marsha Pollard
Provost, Five Towns College

8/29/23

Date

By:

Christopher Kelly
President, Board of Education
Harborfields Central School District

9-30-2023

Date

## EXHIBIT A

FIVE TOWNS COLLEGE
Dual Enrollment Components

The following Five Towns College courses are to be suggested for credit in a dual enrollment agreement with District. Final approval was based upon discussion and agreement with the Chairpersons of the College and the faculty of District.

1. ART101 Art History (3 credits)
2. ART110 Art/Design Theory & Criticism (3 credits)
3. MAC280 Digital Media Art: Design (3 credits)
4. MUS111 Harmony 1 (1 credit)
5. MUS 121 Sight Singing 1 (1 credit)
6. MUS123 Ear Training 1 (1 credit)

## EXHIBIT B

## EDUCATION LAW 2-d RIDER

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

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

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

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

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

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

**Data Security and Privacy Plan**

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

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

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

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

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

**NAME OF PROVIDER: Five Towns College**

**BY:** Marsha Bland **DATED:** 8/29/23

## DATA PRIVACY AND SECURITY PLAN

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

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

FIVE TOWNS COLLEGE

# DATA SECURITY POLICY & PROCEDURES PROGRAM

## The Information Technology (IT) Department

### I. Introduction

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

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

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

### III. Relevant Laws and Regulations

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

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

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

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

## IV. Institutional Initiatives

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

## V. Data Protection and Account Security Measures

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

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

## VI. Institutional Information Risk Assessment and Testing Schedule

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

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

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

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

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

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

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

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

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

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