File Access Error
Local file system access cannot be detected and is required by application.

Web USB Disabled
Web USB cannot be detected and is required by application. It may be disabled or blocked by your security policy.

Example: https://nspirecxii.ti.com/tco/invalid-browser

System Management and Security
TI performs system penetration and application testing. Application testing is performed after code changes. System vulnerability testing is conducted regularly and system intrusion prevention is in place. System software updates and patches are provided as needed. The System, servers and network devices are located in an environmentally controlled and secure facility under controlled circumstances requiring photo ID access by authorized personnel only.

Data Storage, Retention, and Access
All student data at rest is encrypted and hosted on a multi-tenant instance. Data is secured with unique encryption keys for each customer on systems hosting any student data. Data is protected in transit through secure socket layer, hashing, etc.
Beyond the directory level data collected for the purposes of associating an account to a user login managed by 10Duke, TI employees and TI subcontractors do not have access to, will not accept, collect, gather, store, report or record any Personally Identifiable Information at any time. Background checks are completed on personnel, including subcontractors that have access to servers, applications and customer data. TI has a process in place for authenticating callers and resetting access controls. To delete school/system data, requests can be submitted by the Information Request Form.

Development and Change Management Process
Notification to customers regarding any data privacy changes is provided online and users are recommended to periodically check TI's data privacy policy. Updates to the software are provided to customers through an update notice within the software.

Audits and Standards
There is no process for customers to audit the security and privacy of records. TI Security Operations are reviewed and audited by outside groups (Qualys and Nexus). TI follows ISO, NIST and PCI DSS security standards.

Test and Development Environments
Live student/privacy data will not be used in a non-production environment.

Data Breach, Incident Investigation and Response
TI maintains a backup-and-restore and protection processes in the case of a disaster, or denial-of-service attack. TI has a processes for managing a data breach, and in performing security incident investigations and/or e-discovery.

Supplemental Information for Parents' Bill of Rights for Data Privacy and Security

Educational Agency: Broome-Tioga BOCES **("Education Agency")**

Contractor: Texas Instruments Incorporated **("TI")**

Software Product(s):
_____ TI-84™ Plus CE App for Chrome OS™
_____ TI Connect™ for Chrome OS
_____ TI-84™ Plus CE Online Calculator
_____ TI-Nspire™ CX Online Calculator
_____ TI-Nspire™ CX Student software
_____ TI-Nspire™ CX CAS Student software
_____ TI-Nspire™ CX Premium Teacher software
_____ TI-Nspire™ CX II Connect software,
_____ TI-SmartView™ CE emulator for the TI-84 Plus
_____ TI-SmartView™ emulator for MathPrint™ calculators

Contract: TI Student Data Privacy Policy and TI End User License Agreement for the selected software product(s) **("TI Apps"**) identified above.

Contract Term is three (3) years from the date of software activation. (Education Agency to complete after TI Signature).

Activation Date: _____ **End Date:** _____ (3 years from Activation Date)

Exclusive Purpose/Student Data:

TI requires minimal student directory data information to support user verification/authentication to enable use of these **"TI Apps".** This directory information may include the user's name- or alternative identifier, email address, and username/password (collectively **"Student Data").** This directory information is collected by TI (and its subcontractors) from the **Education Agency** for authorized educational/school purposes exclusively to use and support these **TI Apps** for the purposes of associating a **TI App** user account with a **TI App** license and for related support functions. This **Student Data** will not be used for any other purpose. TI does not use **Student Data** to build a student profile or for advertising or marketing purposes. TI will handle this **Student Data** under TI's Student Data Privacy Policy.

Subcontractor Written Agreement:

To support TI's collection and processing of **Student Data** related to these **TI Apps**, TI may use subcontractors (such as 10Duke Software Limited) who are subject to a subcontractor agreement that requires the subcontractors to adhere to materially similar data handling/protection requirements as are imposed on TI by applicable state and federal laws, and as may be required by TI to carry out the practices in this Supplement (and the Contract).

Challenges to Data Accuracy:

If the **Education Agency** or parents deem it necessary to correct any **Student Data** in TI's (and its subcontractor's) possession, TI agrees to facilitate corrections within 45 days of TI's receipt of a written request from the **Education Agency**. The **Education Agency** can contact TI about such request using the Information Request Form link in the TI Student Data Privacy Policy.

Data Transfer and Secure Destruction:

After expiration or termination of the Contract, upon **45** days written request from the **Education Agency**, TI will securely transfer the applicable **Student Data** to the **Education Agency** in a format agreed to by the parties (e.g., csv, pdf, txt secure sftp server, etc.). If no request is made, TI will securely delete and destroy the applicable **Student Data** when TI is aware the **Student Data** is no longer needed for the educational/school purposes described above, or when required under TI's standard data retention policy.

Secure Data Storage:

Student Data will be stored in the United States and protections taken to ensure the **Student Data** will be protected using a third-party cloud or infrastructure (such as Amazon Web Services, Inc.) selected by TI's subcontractor and approved by TI.

Secure Data Security and Privacy Risk Mitigation:

TI deploys policies, processes, and technologies combining selected elements from security policies and standards published by well-known groups or other authoritative sources and applies them to TI's business environment. These include:

- ISO/IEC- 27009:2020 – implementing and maintaining security procedures to detect, protect and respond to cyberattacks that may compromise **Student Data**; and
- NIST Cybersecurity Framework (https://www.nist.gov/cyberframework) – employing reasonable administrative, technical and physical safeguards including: encryption, firewalls, and password protection to protect the security, confidentiality and integrity of **Student Data** from unauthorized disclosure while in motion or in custody.

In addition, TI provides regular and periodic training to its personnel concerning disclosure of personally identifiable information, cybersecurity and practices.

Encryption:

Data will be encrypted while in motion and at rest to prevent interception.

Data Breach:

TI maintains procedures for response to a potential breach of different magnitudes. TI will notify the **Education Agency** of any breach of personally identifiable information within 7 calendar days after its determination the breach has occurred, and the notification will identify any details, to the extent required by law.

Teachers and Principals:

The foregoing data protections will also be extended to personally identifiable information of teachers and principals to the extent required by state and federal laws.

TI gives the **Education Agency** permission to publish this Supplement on its website with a Parents Bill of Rights if the **Student Data** collected by TI is deemed by the **Education Agency** to be personally identifiable information.

Contractor: Texas Instruments Incorporated

Signature: Laura Chambers

Name: Laura de Hoop Chambers

Title: Director, Worldwide Sales and Marketing

Date: 05/05/2023