

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Saratoga Springs City School District

And

ResearchILD

This Data Privacy Agreement ("DPA") is by and between the Saratoga Springs City School District ("EA"), an Educational Agency, and ResearchILD ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of 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:** means 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. **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.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **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.

8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **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.
11. **Release:** Shall have the same meaning as Disclose.
12. **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.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **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.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **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 under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 3/15/24 – 6/30/2027 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (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 Section 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. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA 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. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA 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. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is 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) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and 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 EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall 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) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that 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), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

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

11. Encryption.

Contractor shall 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.

12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and 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 EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

- (b) Notifications required under this paragraph must be provided to the EA at the following address:

David L'Hommedieu

Assistant Superintendent of Information Technology and Operational Innovation & Data Protection Officer

3 Blue Streak Blvd.

Saratoga Springs, NY 12866

D_lhommedieu@saratogaschools.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA 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' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

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

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 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 EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such 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 Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA 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 shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede 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 shall 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 shall be and constitute an original signature, as if all parties had executed a single original document.

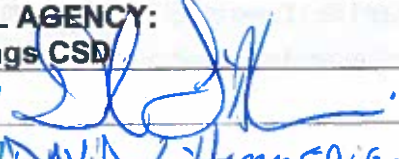
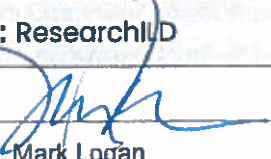
EDUCATIONAL AGENCY: Saratoga Springs CSD	CONTRACTOR: ResearchID
BY: [Signature] 	BY: [Signature] 
[Printed Name] DAVID L. HAMMER	[Printed Name] Mark Logan
[Title] Data Protection Officer	[Title] Executive Director
Date: 4-23-24	Date: April 22, 2024

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

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. 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. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available 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. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at sscsd_dpo@saratogaschools.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR : ResearchILD	
[Signature]	
[Printed Name]	Mark Logan
[Title]	Executive Director
Date:	April 22, 2024

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 Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	ResearchILD
Description of the purpose(s) for which Contractor will receive/access PII	See Attached Description
Type of PII that Contractor will receive/access	Check all that apply: <input type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>May 1, 2024</u> Contract End Date <u>June 30, 2025</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires 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 Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input checked="" type="checkbox"/> Other:</p> <p>ResearchILD does not collect PII</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
Encryption	Data will be encrypted while in motion and at rest.


CONTRACTOR : ResearchILD	
[Signature]	
[Printed Name]	Mark Logan
[Title]	Executive Director
Date:	April 22, 2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) 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. For every contract, 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. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See Attached.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, 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 EA.	
6	Describe how data will be transitioned to the EA 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 EA.	
8	Outline how your data security and privacy program/practices align with the EA'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.	PLEASE 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.	See Attached Description
	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.	
	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	

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	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.	
	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.	
	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.	
	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.	
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	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.	
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	

Function	Category	Contractor Response
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	



RESEARCH INSTITUTE FOR
LEARNING & DEVELOPMENT

SMARTS PRODUCTS TERMS OF USE, PRIVACY POLICY & SYSTEM SECURITY INFORMATION

The following SMARTS Products Terms of Use, Privacy Policy and System Security Information apply to any and all licensed users of the Research Institute for Learning and Development ("ResearchILD") products, services and/or websites. Such licensed users are hereinafter referred to as LICENSEES as defined in the SMARTS Product Terms of Use Section below.

SMARTS PRODUCTS TERMS OF USE

ResearchILD operates various websites (the "Websites"), including but not limited to the Websites available at www.researchild.org and www.smarts-ef.org, and provides certain content, curriculum products and services to users of the Websites. In addition to these SMARTS Product Terms of Use, Privacy Policy and System Security Information, LICENSEES agree to be bound by the ResearchILD Website Terms of Use also posted on the Websites.

The SMARTS programs, including but not limited to the SMARTS Secondary, SMARTS Premium, SMARTS Elementary, SMARTS@Home and MetaCOG Survey and Toolkit curriculum products, and all related training, workshops, lectures, presentations, research findings, publications, concepts, ideas, exercises, graphics, explanations, and/or all materials available via ResearchILD's Websites and any and all other formats are the exclusive property of ResearchILD. Hereinafter all such materials will be referred to as the "SMARTS Curriculum" or "SMARTS".

Only an authorized individual(s) may utilize the SMARTS Curriculum. An authorized individual ("LICENSEE") is someone who has an up-to-date, fully paid individual, clinic, or school license to use specified curriculum product(s), (e.g., SMARTS Secondary or Premium, SMARTS Elementary, SMARTS@Home, and/or MetaCOG). All Licenses must be renewed on an annual basis or as specified in the product purchase information.

To access the specified SMARTS Curriculum product, each LICENSEE must have an individual license assigned by ResearchILD via a unique LICENSEE name and password. If the license is purchased by a school or other organization on behalf of a LICENSEE, the license may be reassigned to another LICENSEE during the license term by contacting ResearchILD to cancel access and request a new LICENSEE name and password.

SMARTS Curriculum licenses **may not be shared or used by more than one LICENSEE**. The SMARTS Curriculum may be used solely for LICENSEE'S students and/or clients. SMARTS may not be distributed, shared, copied or made available for use by anyone other than the authorized LICENSEE. If the LICENSEE has a license assigned by LICENSEE'S school or other organization, SMARTS may be utilized solely for such school's/organization's students. The school/organization that purchased the license(s) is responsible for ensuring all LICENSEES are made aware of and comply with these Intellectual Property terms.

LICENSEE may **NOT** utilize the SMARTS Curriculum in the following manner without specific written permission from ResearchILD:

- With students and/or clients as part of an on-line education program, virtual school, or any

other remote access program or service with the following exception. Subject to the other Terms of Use included herein, a LICENSEE may upload SMARTS materials to their own electronic classroom for use with their students.

- As part of a training program or course for teachers, psychologists, educational therapists and/or other applicable professions.
- Any other manner not expressly permitted under these Terms of Use.

Use of the SMARTS materials is subject to the Terms of Use described herein. By using any or all of the SMARTS materials, LICENSEE is acknowledging that LICENSEE has read, understood and agreed to be bound by these Terms of Use. If LICENSEE does not agree to these Terms of Use, LICENSEE should not utilize the materials.

SMARTS materials may only be utilized in their original form with all trademarks, logos and intellectual property language intact. Any permitted use of SMARTS content not in its original form must be clearly identified and have the following reference language included in a visible location: "©2014-2023 ResearchILD. All rights reserved. Use is by permission only."

LICENSEE may **NOT**: a) modify, b) make improvements, and/or c) create derivative works or adjusted versions of SMARTS (hereinafter referred to as "Modifications") without written permission from ResearchILD. In the event that LICENSEE makes Modifications to SMARTS, LICENSEE hereby acknowledges and agrees that such Modifications: a) must be immediately provided to ResearchILD and b) shall become the exclusive property of ResearchILD. LICENSEE does not retain any ownership or other rights in the Modifications except for the limited, non-transferable license to use the Modifications in accordance with these Terms of Use. Notwithstanding the foregoing, LICENSEE may customize individual handouts or slides for use with LICENSEE's students/clients only.

PRIVACY POLICY

ResearchILD shall only use LICENSEE information collected or received solely for the operation of ResearchILD, the Websites and/or the provision of Products and Services and in accordance with the Websites Terms of Use and SMARTS Product Terms of Use. ResearchILD shall not share LICENSEE information with third parties outside of ResearchILD and its related organizations except as noted below.

- ResearchILD may share LICENSEE's information with third-party business partners for the purpose of providing a service or product to LICENSEE. Third-party business partners will be given limited access to LICENSEE's information as is reasonably necessary to deliver the product or service, e.g., to ship an order.
- ResearchILD may share aggregated demographic information with third-party business partners. This is not linked to any personal information that can identify any individual person and/or LICENSEE.

ResearchILD may use the information collected or received, such as LICENSEE's email address, to communicate directly with LICENSEE. ResearchILD may send LICENSEE emails containing newsletters, information about product and services, and special offers. If LICENSEE does not want to receive such email messages, LICENSEE will be given the option to opt out or change LICENSEE's preferences. ResearchILD shall also use LICENSEE's information to send LICENSEE service-related emails (e.g., account verification, purchase and billing confirmations and reminders, changes/updates to features of the service, technical and security notices). LICENSEE may not opt out of service-related emails.

The Websites automatically collect some technical information from LICENSEES in order to give LICENSEE the best possible experience. ResearchILD uses web measurement technology (Google Analytics) to automatically track LICENSEE interactions with the Products and Services. This information is only used to help ResearchILD make the Products and Services more useful for LICENSEE. ResearchILD does not track or record personally identifiable information about individual LICENSEES and their visits.

A cookie may also be generated to optimize LICENSEE's experience on the Websites, allowing LICENSEE to have repeat access to the free lesson and/or purchased lessons on LICENSEE's computer without re-entering LICENSEE's information. LICENSEE can turn off the use of cookies at any time by changing LICENSEE's specific browser settings.

Any content that LICENSEE voluntarily discloses for posting to the Websites such as our Message Board or Subscriber Community ("LICENSEE Content") becomes available to the public and cannot be removed, except by ResearchILD in our sole discretion. Once posted on the Website, however, LICENSEE Content may not be removable from public view, as copies may remain viewable in cached and archived pages of the service, on other Websites that have republished ResearchILD, or if other LICENSEES have copied or saved that information. If LICENSEE does not wish LICENSEE's LICENSEE Content to be available to the public, please don't post it on the Website.

ResearchILD take precautions to protect LICENSEE's sensitive information. When LICENSEE submit sensitive information via the Websites, LICENSEE's information is protected both online and offline.

- Wherever ResearchILD collects sensitive information (such as credit card data), that information is encrypted and transmitted to ResearchILD in a secure way. LICENSEE can verify this by looking for a lock icon in the address bar and looking for "https" at the beginning of the address of the Web page.
- While ResearchILD use encryption to protect sensitive information transmitted online, ResearchILD also protects LICENSEE's information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information. The computers/servers in which ResearchILD stores personally identifiable information are kept in a secure environment.
- In the event that any information under our control is compromised as a result of a breach of security, ResearchILD will take reasonable steps to investigate the situation and where appropriate, notify those individuals whose information may have been compromised and take other steps, in accordance with any applicable laws and regulations.

The MetaCOG Survey and Toolkit product, also available as part of SMARTS Premium Curriculum, enables the LICENSEE and LICENSEE'S students to complete surveys online. Students answer questions about their learning style and strategy use. The information gathered from the MetaCOG enables the educator to target the use of the SMARTS curriculum lessons to the learning challenges identified in the MetaCOG survey. **NO STUDENT IDENTIFYING INFORMATION OR STUDENT DATA IS COLLECTED IN THE SURVEY.**

Use of the MetaCOG Survey feature by the educator is voluntary and not necessary for utilizing the SMARTS Curriculum materials. LICENSEE In utilizing the MetaCOG survey, educators are instructed to use student identifiers (e.g., id numbers, initials) rather than student names. It is the responsibility of the LICENSEE to only use the MetaCOG survey tool in accordance with their school's privacy policy as well as any applicable privacy laws. Each MetaCOG LICENSEE shall only have access to the data entered by their own students, and may not view data entered by students associated with another LICENSEE. In the event ResearchILD becomes aware that any MetaCOG data has been inappropriately accessed, ResearchILD will take reasonable steps to investigate and if appropriate, notify the LICENSEE.

The Websites may contain links to other third-party websites. Please be aware that ResearchILD is not responsible for the content or privacy practices of such other third-party websites. ResearchILD encourages LICENSEEs to be aware when using these links and to read the privacy statements of such third-party websites.

SMARTS PRODUCTS SYSTEMS SECURITY INFORMATION

SMARTS Curriculum Product Description: The SMARTS Products are delivered on a subscription basis that gives licensed users access to the curriculum materials online via the educator's email and a password.

The SMARTS Products consists primarily of instruction materials, lesson plans, student handouts and presentations in PDF and MS PowerPoint (PPT) formats, that the educator downloads as needed. Educators do not need to provide any student data to use these materials in their classrooms.

There is only one feature available as part of the SMARTS Premium product or as separate product known as the MetaCOG Survey and Toolkit, that enables students to input information directly into the program. This feature enables the educator to obtain information that can be used to target the SMARTS curriculum lessons to the learning challenges identified by their students. Students are asked to provide an identifier (e.g., their initials or a student code) and answer questions about their learning style and strategy use. Use of the MetaCOG Survey feature by the educator is voluntary and not necessary for utilizing the SMARTS materials. In utilizing the MetaCOG survey, educators are instructed to use student identifiers rather than the name. No student identifying information or student data is collected in the survey.

Assigning SMARTS Licenses: Accounts are assigned to each LICENSEE by using the educator's email and a unique password. Only the educator's work email is used for assigning SMARTS Licenses. No personally identifiable information is collected for use of the SMARTS Products.

Data Storage and Security: SMARTS data is stored and managed through the SiteGround platform. For SiteGround server locations, see: https://www.siteground.com/kb/where_are_sitegrounds_servers/

Access to data and SiteGround server access is limited to ResearchILD administrative and IT staff, as necessary for the management of the specific survey data. Two-factor authentication is enabled where available and enforced for administrators and strong passwords are required for all staff with access per current security standards. ResearchILD practices are in compliance with the NIST Cybersecurity Framework Version 1.1

The Websites operate on a secure Wordfence server, with SSL (Secure Sockets Layer) certificates installed which enable an encrypted connection between the secure server and a user's web browser.

ResearchILD utilizes WordPress plugins to support the administrative functionality of the site, including PaidMembershipPro and Gravity Forms, however none of these plugins are utilized/related to the direct

use of the SMARTS product by LICENSEES. Plugins are updated monthly by a designated staff member.

In the event of a data breach, ResearchILD would notify the account contact even though no educator or student identifying data is collected other than the educator's email.

Operating system requirements: There are no operating system requirements or integrations necessary to use the SMARTS Products. The SMARTS curriculum is an online product accessible through the internet. Use of PowerPoint materials does require access to Microsoft Office Suite; however, they can also be opened using a program such as Google Slides. In addition, some of ResearchILD's training videos for educators and optional content videos for students are hosted on YouTube.

Any questions about these SMARTS PRODUCTS TERMS OF USE, PRIVACY POLICY & SYSTEM SECURITY INFORMATION and/or requests for further information should be directed to ResearchILD, 4 Militia Drive, Suite 20, Lexington, MA 02421, telephone: 781-861-3711, email: info@researchild.org.

