PHIT Kids Academy – School Data Privacy Agreement

SCHOOL DATA PRIVACY AGREEMENT (DPA)

This School Data Privacy Agreement ("Agreement") is entered into by and between **PHIT America, Inc.**, a nonprofit organization with its principal place of business at 1032 15th St. NW, Suite 108, Washington DC 20005 and **[School District / School Name]**, with its principal place of business at [ADDRESS] ("Educational Agency" or "School").

This Agreement governs Provider's access to, use of, and protection of Student Data in connection with the provision of **PHIT Kids Academy** and related services (the "Services").

---

1. PURPOSE AND SCOPE

The Services provide age-appropriate physical activity, wellness, and sports education content for use in K-12 educational settings. This Agreement is intended to ensure compliance with applicable student data privacy laws, including the **Family Educational Rights and Privacy Act (FERPA)** and the **Children's Online Privacy Protection Act (COPPA)**.

Provider acts as a **School Official** under FERPA with a legitimate educational interest in the Student Data processed solely for the purpose of delivering the Services.

---

2. DEFINITIONS

- **"Student Data"** means any information that is directly related to an identifiable student and provided by or on behalf of the School, including but not limited to student identifiers, class-level participation data, or access credentials.
- **"Personal Information"** shall have the meaning set forth in COPPA.
- **"De-Identified Data"** means data that has been stripped of all personally identifiable information and cannot reasonably be used to identify a student.

---

3. COMPLIANCE WITH FERPA

Provider agrees that:

- Student Data shall be used **solely for educational purposes** authorized by the School;

- Provider shall not disclose Student Data to any third party except as permitted under this Agreement or required by law;
- Provider shall not use Student Data for advertising, marketing, or profiling;
- Upon request, Provider shall assist the School in responding to parental or eligible student requests regarding access to or correction of education records.

---

4. COMPLIANCE WITH COPPA

To the extent the Services are directed to children under the age of 13:

- The School provides consent on behalf of parents solely for educational use, pursuant to the COPPA school consent exception;
- Provider does **not require students to create individual accounts**;
- Provider does **not knowingly collect Personal Information directly from children**;
- Any limited information processed is used exclusively to provide the Services and is protected in accordance with this Agreement.

---

5. DATA COLLECTION AND MINIMIZATION

Provider agrees to collect and process only the **minimum data necessary** to deliver the Services. The Services are designed so that:

- Students consume content without submitting personal data;
- Teachers or administrators manage access and participation;
- No student-generated content (photos, videos, chat, or free-text responses) is required.

---

6. DATA OWNERSHIP AND CONTROL

- All Student Data remains the property of the School or the applicable student/parent;
- Provider acquires no ownership rights in Student Data;
- Provider shall comply with all lawful instructions from the School regarding Student Data.

---

7. DATA SECURITY

Provider shall implement and maintain commercially reasonable administrative, technical, and physical safeguards to protect Student Data, including:

- Encryption of data in transit;
- Role-based access controls;
- Limited staff access based on necessity;
- Secure hosting environments maintained by reputable third-party providers.

---

8. SUB-PROCESSORS

Provider may use the following sub-processors solely to deliver the Services:

- Website platform (e.g., Wix)
- Payment processor (e.g., Stripe – adult accounts only)
- Video hosting provider (e.g., Vimeo – private, domain-restricted)
- Community or communication platform (if applicable, adult-managed only)

Provider shall ensure that all sub-processors are contractually obligated to protect Student Data consistent with this Agreement.

---

9. DATA RETENTION AND DELETION

- Provider shall retain Student Data only for the duration of the Services or as required by law;
- Upon termination of services or written request by the School, Provider shall securely delete or return Student Data within a reasonable time frame, unless retention is legally required.

---

10. DATA BREACH NOTIFICATION

In the event of a confirmed data breach involving Student Data, Provider shall:

- Notify the School without unreasonable delay;
- Provide information reasonably necessary for the School to comply with applicable notification obligations;
- Cooperate with remediation efforts.

---

11. AUDIT AND COMPLIANCE

Upon reasonable notice, Provider shall make available information necessary to demonstrate compliance with this Agreement and applicable privacy laws.

---

12. TERM AND TERMINATION

This Agreement shall remain in effect for the duration of the Services. Upon termination, Provider's obligations regarding Student Data shall survive until all data is properly deleted or returned.

---

13. GOVERNING LAW

This Agreement shall be governed by the laws of the state in which the School is located, without regard to conflict of law principles.

---

14. ENTIRE AGREEMENT

This Agreement constitutes the entire understanding between the parties with respect to Student Data privacy and supersedes any prior agreements on this subject.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the dates set forth below.

PHIT America, Inc.
By: _____
Name: _____
Title: _____
Date: _____

[School District / School Name]
By: _____
Name: _____
Title: _____
Date: _____

APPENDIX A – DATA SECURITY OVERVIEW

PHIT America implements administrative, technical, and physical safeguards designed to protect Student Data from unauthorized access, disclosure, alteration, or destruction.

Administrative Safeguards

- Staff access limited to authorized personnel with a legitimate need
- Annual review of data protection practices
- Incident response procedures in place

Technical Safeguards

- Encryption of data in transit (HTTPS/TLS)
- Secure authentication for administrative users
- Reputable cloud hosting infrastructure

Physical Safeguards

- No on-premises storage of Student Data
- Data hosted in professionally managed data centers

APPENDIX B – SUB-PROCESSOR LIST

PHIT America utilizes the following sub-processors solely to deliver the Services:

- **Website Platform**: Wix (content delivery, access control)
- **Video Hosting**: Vimeo (private, domain-restricted video streaming)
- **Payment Processing**: Stripe (adult, school, or parent accounts only)
- **Email & Communications**: [e.g., ZOHO / approved provider]

All sub-processors are contractually obligated to maintain safeguards consistent with this Agreement.

APPENDIX C – DATA RETENTION POLICY

- Student Data is retained only for the duration necessary to provide the Services.
- No long-term individual student profiles are maintained.
- Upon termination or written request, data is securely deleted or de-identified.

APPENDIX D – SCHOOL PRIVACY SUMMARY (ADMINISTRATOR-FACING)

Do students create accounts?
No. Access is managed by schools or teachers.

Is data used for marketing or advertising?
No. Never.

Is data sold or shared?
No. Data is used only to provide educational services.

Is the platform COPPA compliant?
Yes. The platform relies on school-based consent and does not collect personal data directly from children.

APPENDIX E – PUBLIC STUDENT PRIVACY STATEMENT (SUMMARY)

PHIT Kids Academy is designed for educational use and does not require students to submit personal information. The program provides safe, age-appropriate physical activity and sports education content without advertising, tracking, or social media features.

PHIT America complies with FERPA and COPPA and works directly with schools and parents to protect student privacy.

1. **Appendix C – Data Retention Policy**
   Clear statements around minimization, deletion, and de-identification.
2. **Appendix D – School Privacy Summary (Admin-Facing)**
   One-page style language districts can circulate internally.
3. **Appendix E – Public Student Privacy Statement**
   Language suitable for your website that aligns tightly with the DPA.

Recommended next refinements (when you're ready)

- Create a **California SOPIPA addendum** (often requested first)
- Add a **"No AI Training / No Biometric Data" clause** (even if not used)
- Convert Appendix D into a branded **1-page PDF handout**

- Prepare a **district onboarding checklist** for superintendents and IT directors