

DATA PROTECTION ADDENDUM

BETWEEN: Fauquier County Public Schools ("District") and (Vendor name/address): Focused Fitness 2426 S Dishman Ave Spokane, WA 99209
Goods/Service: WELNET Software

This Data Protection Addendum ("Addendum") is to be attached and be part of all purchase orders and contracts where the Vendor provides goods or services which necessitate that the Vendor create, obtain, transmit, use, maintain, process, or dispose of District Data (as defined in the Definitions section (Exhibit "A") of this Addendum) in order to fulfill its obligations to the District. Given the critical nature of Student Data and Information, this Addendum, once fully executed, shall be incorporated into and become part of the Service Agreement, even if not specifically referenced in that Service Agreement.

The purpose of this Addendum is to describe the duties and responsibilities to protect student data transmitted to Provider from the District pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including but not limited to the FERPA, PPRA, COPPA, HIPPA, and the Code of Virginia § 22.1-289.01.

1. **Nature of Services Provided.** The Vendor has agreed to provide the following digital educational services described as outlined in Exhibit "B" hereto:
2. **Data to Be Provided.** In order to perform the Services described in the Service Agreement, District shall provide the categories of data described as indicated in the Schedule of Data, attached hereto as Exhibit "C".
3. **Rights and License in and to District Data.** The parties agree that as between them, all rights including all intellectual property rights in and to District Data shall remain the exclusive property of the District, and Vendor has a limited, nonexclusive license as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give Vendor any rights, implied or otherwise, to District Data, content, or intellectual property, except as expressly stated in the Agreement.
4. **Intellectual Property Rights/Disclosure.**
 - 8.1. Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by Vendor (or its subcontractors) for the District will not be disclosed to any other person or entity.
 - 8.2. Vendor warrants to the District that the District will own all rights, title and interest in any and all intellectual property created in the performance of this Agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all district-created intellectual property created in the performance of this Agreement to the District, and will execute any future assignments or other documents needed for the District to document, register, or otherwise perfect such rights.

- 8.3. Notwithstanding the foregoing, for grant collaboration pursuant to subcontracts under sponsored grants, intellectual property rights will be governed by the terms of the grant or contract to the District to the extent such grant or contract requires intellectual property terms to apply to subcontractors.
5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.
6. **Parent Access.** Provider and the District shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the District's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the District, who will follow the necessary and proper procedures regarding the requested information.
7. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the District. Provider shall notify the District in advance of a compelled disclosure to a Third Party unless legally prohibited.
8. **Data Privacy.**
- 8.1. Vendor shall use District Data only for the purpose of fulfilling its duties under this Agreement and will not share such data, including anonymized data, with or disclose it to any third party without the prior written consent of the District, except as required by law.
- 8.2. District Data will not be stored or processed outside the United States without prior written consent from the District.
- 8.3. Vendor shall provide access to District Data, including anonymized only to its employees and subcontractors who need to access the data to fulfill Vendor obligations under this Agreement. Vendor shall ensure that employees and subcontractors who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement. If Vendor shall have access to "education records" for the District's students as defined under the Family Educational Rights and Privacy Act (FERPA), the Vendor acknowledges that for the purpose of this Agreement it may be designated as, and acting in the capacity of, a "school official" with "legitimate educational interests" in the District Education records, as those terms have been defined under FERPA and its implementing regulations, and the Vendor agrees to abide by the FERPA limitations and requirements imposed on school officials. Vendor shall use the Education records only for the purpose of fulfilling its duties under this Agreement for District's and its End User's benefit, and will not share such data with or disclose it to any third party

except as provided in this Agreement, required by law, or authorized in writing by the District.

8.4. Vendor shall not use District Data (including metadata) for advertising or marketing purposes unless such use is specifically authorized by this agreement or otherwise authorized in writing by the District.

8.5. Vendor agrees to assist District in maintaining the privacy of District's Data as may be required by State and Federal law, including but not limited to the Protection of Pupil Rights Amendment (PPRA), The Children's Online Privacy Protection Act (COPPA), and the Government Data Collection and Dissemination Practices Act of Virginia.

9. Data Security.

9.1. Vendor shall store and process District Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all electronic District Data will be encrypted in transmission using SSL (Secure Sockets Layer) (including via web interface) and stored at no less than 128-bit level encryption.

9.2. Vendor shall use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement.

10. Employee and Subcontractor Qualifications.

10.1. Vendor shall ensure that its employees and subcontractors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this agreement including but not limited to all terms relating to data and intellectual property protection.

10.2. If the Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of District Data known as Personally Identifiable Information or financial or business data which has been identified to the Vendor as having the potential to affect the accuracy of the District's financial statements, Vendor shall perform the following background checks on all employees who have potential to access such data in accordance with the Fair Credit Reporting Act Social Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC). The District reserves the right to request verification that the Vendor has performed the required background checks.

11. Data Authenticity and Integrity. Vendor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity. Vendor shall be responsible for ensuring that District Data is retrievable in a format that can be easily read in compliance with the General Schedules of the Library of Virginia, but not limited to, General Schedules 02, 19 and 21 of the Library of Virginia in accordance with § 42.1-85, of the Code of Virginia.

12. Security Breach.

12.1. Response. Immediately upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of District Data, Vendor shall notify the District in accordance with Section 22, fully investigate the incident, and cooperate fully with the District's Investigation of and response to the incident. Vendor shall follow the following process:

12.1.1. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

12.1.2. The security breach notification described above in section 10(a) shall include, at a minimum, the following information:

12.1.2.1. The name and contact information of the reporting District subject to this section.

12.1.2.2. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

12.1.2.3. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

12.1.2.4. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

12.1.2.5. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

12.1.3. At District's discretion, the security breach notification may also include any of the following:

12.1.3.1. Information about what the agency has done to protect individuals whose information has been breached.

12.1.3.2. Advice on steps that the person whose information has been breached may take to protect himself or herself.

12.1.4. Except as otherwise required by law, Vendor shall not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the District.

- 12.2. **Liability.** In addition to any other remedies available to the District under law or equity, Vendor shall reimburse the District in full for all costs incurred by the District in investigation and remediation of any Security Breach caused in whole or in part by Vendor or subcontractors, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed against the District as a result of the Security Breach.

13. Response to Legal Orders, Demands or Requests for Data.

- 13.1. Except as otherwise expressly prohibited by law, Vendor shall:
 - 13.1.1 immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking District Data;
 - 13.1.2 consult with the District regarding its response;
 - 13.1.3 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
 - 13.1.4 upon the District's request, provide the District with a copy of its response.
- 13.2. If the District receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act) ("requests") or request seeking District Data maintained by Vendor, the District will promptly provide a copy of the request to Vendor. Vendor shall promptly supply the District with copies of records or information required for the District to respond, and will cooperate with the District's reasonable requests in connection with its response.

14. Data Transfer Upon Termination or Expiration.

- 14.1. Upon termination or expiration of this Agreement, Vendor shall ensure that all District Data are securely returned or destroyed as directed by the District. Transfer to the District or a third party designated by the District shall occur within 30 days, and without significant interruption in service. Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. In the event that the District requests destruction of its data, Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Vendor might have transferred District data. The Vendor agrees to provide documentation of data destruction to the District.

14.2. Vendor shall notify the District of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the District access to Vendor's facilities to remove and destroy District- owned assets and data. Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the District. Vendor shall also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the District. Vendor shall work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the District, all such work to be coordinated and performed in advance of the formal, transition date.

15. **Audits.**

15.1. The District reserves the right in its sole discretion to perform audits of Vendor at the District's expense to ensure compliance with the terms of this Agreement. The Vendor shall reasonably cooperate in the performance of such audits. This provision applied to all agreements under which the Vendor must create, obtain, transmit, use, maintain, process, or dispose of District Data.

15.2. If the Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of District Data known as Personally Identifiable Information or financial or business data which has been identified to the Vendor as having the potential to affect the accuracy of the District's financial statements, Vendor shall at its expense conduct or have conducted at least annually:

- (1) American Institute of CPSSs Service Organization Controls (SOC) Type II audit, or other security audit with audit objective deemed sufficient by the District, which attests the Vendor's security policies, procedures and controls;
- (2) vulnerability scan, performed by a scanner approved by the District, of Vendor's electronic systems and facilities that are used in any way to deliver electronic service under this Agreement; and
- (3) formal penetration test, performed by a process and qualified personnel approved by the District, of Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement.

15.3. The Vendor shall provide the District upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement. The District may require, at District expense, the Vendor to perform additional audits and tests, the results of which will be provided promptly to the District.

- 16. Institutional Branding.** Each party shall have the right to use the other party's Brand Features only in connection with performing the functions provided in this Agreement. Any use of a party's Brand Features will inure to the benefit of the party holding intellectual property rights in and to those features.
- 17. Compliance.**
- 17.1. Vendor shall comply with all applicable laws and industry standards in performing services under this Agreement. Any Vendor personnel visiting the District's facilities will comply with all applicable District policies regarding access to, use of, and conduct within such facilities. The District will provide copies of such policies to Vendor upon request
- 17.2. Vendor warrants that any subcontractors used by Vendor to fulfill its obligations under this agreement will be subject to and will comply with each and every term of this Data Protection Addendum in the same manner that Vendor itself is subject to the terms of this Data Protection Addendum.
- 17.3. Vendor warrants that the service it will provide to the District is fully compliant with and will enable the District to be in compliance with relevant requirements of all laws, regulation, and guidance applicable to the District and/or Vendor, including but not limited to: the Children's Online Privacy Protection Act (COPPA); Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act. (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Protection of Pupil Rights Amendment (PPRA); Americans with Disabilities Act (ADA), and Federal Export Administration Regulations.
- 18. Conflict Other Agreements Between the Parties.** If there is any conflict or potential conflict between the terms of this Data Protection Addendum and the terms of any other agreements between the parties, the terms of this Data Protection Addendum shall control.
- 19. No End User Agreements.** In the event that the Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with District employees or other End Users, the District may request that such agreements shall be null, void and without effect, and the terms of this Agreement shall apply.
- 20. Terms and Terminations.**
- 20.1. Term. This Addendum will become effective when the Vendor accepts the Purchasing Terms and Conditions and is issued a Purchase Order for goods or services or receives payment by purchase card or check which necessitate that the Vendor create, obtain, transmit, use, maintain, process, or dispose of District Data in order to fulfill its obligations to the District. It will continue in effect until all obligations of the Parties have been met, unless terminated as provided in this

section. In addition, certain provisions and requirements of this Addendum will survive its expiration or other termination in accordance with Section 19 herein.

20.2. **Termination by the District.** The District may immediately terminate the Agreement if the District makes the determination that the Vendor has breached a material term of this Data Protection Addendum.

20.3. **Automatic Termination.** This Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Agreement between the Parties.

21. **Survival.** The Vendor's obligations under Section 14 shall survive termination of this Agreement until all District data has been returned or securely destroyed.

22. **Notices.** Any notices to be given will be made via certified mail or express courier to the address given below, except that notice of a Security Breach shall also be given as provided in Section 12. of this Addendum.

22.1. If to the Vendor:

COMPANY NAME, CONTACT NAME, and ADDRESS as listed on the Purchase Order

22.2. If to the District:

Louis McDonald, Director of Technology
Fauquier County Public Schools
320 Hospital Drive, Suite 40
Warrenton, VA 20186
Telephone: 540-422-7013
Email: Louis.McDonald@fcps1.org

22.3. With a copy to:

Susan Monaco, Procurement Manager
Fauquier County Govt/Public Schools Procurement Div.
320 Hospital Drive, Suite 23
Warrenton, VA 20186
Telephone: 540-422-8348
Email: Susan.Monaco@fauquiercounty.gov

22.4. If notice concerns a Security Breach:

Louis McDonald
Director of Technology Services
Fauquier County Public Schools
320 Hospital Drive, Suite 40
Warrenton, VA 20186
Telephone: 540-422-7013
Email: Louis.McDonald@fcps1.org

- 23. **Advertisement.** Any and all forms of advertisement, directed towards children, parents, guardians or District employees, as a result of this Agreement, shall be strictly prohibited.
- 24. **Governing Law.** This Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Virginia, excluding its choice of law rules. Any action or proceeding seeking any relief under or with respect to this Agreement shall be brought solely in the Circuit Court for Fauquier County, Virginia.
- 25. **Indemnification.** Vendor shall indemnify, defend and hold harmless District and District's affiliates, officers, directors, and employees from and against any third-party claims, demands, causes of action, judgments, damages, liabilities, costs and expenses (including reasonable attorney's fees) arising from or relating to Vendor's or any of Vendor's employees, agents, contractors, or representatives unauthorized use, misuse, or illegal use of District Information or De-identified Information or any breach of this Agreement by Vendor. The District and any indemnified party shall cooperate and comply with the reasonable requests of Vendor in connection with the defense of any such claim. The receipt or providing such assistance is not a waiver of any alleged breach nor does the acceptance of such assistance constitute a waiver of any such breach by the District. Vendor shall control the defense and settlement of any such claim.

SO AGREED:

FAUQUIER COUNTY PUBLIC SCHOOL BOARD

BY: Susan R. Monaco
Title: FCS Procurement Manager
Date: 8/29/17

VENDOR NAME: Focused Fitness

BY: [Signature]
Title: VP-Software
Date: 8-29-17

Designated as School Official Yes NO (filled in by District)
SM 8/29/17

EXHIBIT "A"

DEFINITIONS

- a. **"Agreement, Service or otherwise"** means any contractually binding document signed by the Vendor and the District legally obligating both parties; also referred to as "Contract", "Software Agreement", "Purchase Agreement".
- b. **"Brand Features"** means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.
- c. **"District"** means Fauquier County Public School Division.
- d. **"District Data"** includes all Personally Identifiable Information and other information that is not intentionally made generally available by the District on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and student, employees, and personnel data and metadata.
- e. **"Elementary and secondary school purposes"** means purposes that (i) customarily take place at the direction of an elementary or secondary school, elementary or secondary school teacher, or school division; (ii) aid in the administration of school activities, including instruction in the classroom or at home; administrative activities; and collaboration between students, school personnel, or parents; or (iii) are otherwise for the use and benefit of an elementary or secondary school.
- f. **"End User"** means the individuals authorized by the District to access and use the Services provided by the Vendor under this Agreement.
- g. **"Personally Identifiable Information"** (or PII) includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "personal information" as defined in § 2.2-3801 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; "health records" as defined in § 32.1- 127.1:03B of the Code of Virginia; "directory information" as defined by § 22.1-287.1 of the Code of Virginia; "medical information" as defined by § 32.1-127.05A of the Code of Virginia "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal- identification numbers such as passport, visa or state identity card numbers.
- h. **"Personal profile"** does not include account information that is collected and retained by a school service provider and remains under control of a student, parent, or elementary or secondary school.

- i. **"School-affiliated entity"** means any private entity that provides support to a local school division or a public elementary or secondary school in the Commonwealth. "School-affiliated entity" includes alumni associations, booster clubs, parent-teacher associations, parent-teacher-student associations, parent-teacher organizations, public education foundations, public education funds, and scholarship organizations.
- j. **"School service"** means a website, mobile application, or online service that (i) is designed and marketed primarily for use in elementary or secondary schools; (ii) is used (a) at the direction of teachers or other employees at elementary or secondary schools or (b) by any school-affiliated entity; and (iii) collects and maintains, uses, or shares student personal information. "School service" does not include a website, mobile application, or online service that is (a) used for the purposes of college and career readiness assessment or (b) designed and marketed for use by individuals or entities generally, even if it is also marketed for use in elementary or secondary schools.
- k. **"School service provider"** means an entity that operates a school service pursuant to a contract with a local school division in the Commonwealth.
- l. **"Securely Destroy"** means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards of Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.
- m. **"Security Breach"** means an event in which District Data is exposed to unauthorized disclosure, access, alteration, or use.
- n. **"Services"** means any goods or services acquired by the District from the Vendor, including computer software, mobile applications (apps), and web-based tools accessed by students and/or their parents via the Internet and used as part of the school activity.
- o. **"Student personal information"** means information collected through a school service that identifies a currently or formerly enrolled individual student or is linked to information that identifies a currently or formerly enrolled individual student.
- p. **"Targeted advertising"** means advertising that is presented to a student and selected on the basis of information obtained or inferred over time from such student's online behavior, use of applications, or sharing of student personal information. "Targeted advertising" does not include advertising (i) that is presented to a student at an online location (a) on the basis of such student's online behavior, use of applications, or sharing of student personal information during his current visit to that online location or (b) in response to that student's request for information or feedback and (ii) for which a student's online activities or requests are not retained over time for the purpose of subsequent advertising.

EXHIBIT "B"

DESCRIPTION OF SERVICES

TO BE COMPLETED BY VENDOR. VENDOR NAME: Focused Fitness/WEINER

[INSERT DETAILED DESCRIPTION OF SERVICES HERE]

See following pages



FOCUSED FITNESS

Sensible Fitness and Health Programs for Today's Kids

WELNET® DS (District Solution)

Detailed Information

WELNET® DS is a web-based software program used district-wide to assess fitness and health through a collection of modules. WELNET® DS enables educators to measure the five components of physical fitness, check for understanding of fitness and health concepts, track health-related habits and behaviors. WELNET® DS provides analysis of longitudinal data trends and supports improved instruction, student learning and personal fitness.



WELNET® DS will simplify the process of gathering student data while providing longitudinal data. Teachers and administrators can print individual and group reports and analyze results from any internet-enabled device. WELNET® DS also exports data in formats suitable for researchers and evaluators to analyze. Focused Fitness provides the hosting and support so there is no servers or hardware to purchase or maintain. All module enhancements are made available to all current users at no additional cost so there is never a need to install new versions.

Hardware / Software Requirements

- Can be accessed by students, parents or teachers with any internet-enabled device
- Supported operating systems: Windows, Macintosh, Linux
- Supported browsers:
 - Windows: Internet Explorer 9, 10,11 and Edge, Firefox, Chrome
 - OS X (MAC): Safari, Chrome
- Mobile-Responsive design allows for use on any size screen
- No installation required - no computer server to purchase or software version to install
- Telephone and email support for all teachers and administrators available – no additional district technical support necessary

Program Design

- Simple, consistent user interface between all modules
- Usable by novice and experienced users
- Four view levels: district, building, teacher, student/parent level



FOCUSED FITNESS

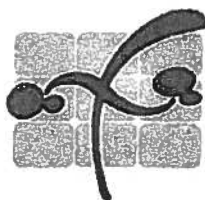
Sensible Fitness and Health Programs for Today's Kids

Fitness Measurement Module

- Fitness measurements and standards are customizable – districts may choose any combination of fitness measurements
- Fitness measurements can be different for various levels
- Automatically calculated values can be included: BMI, VO2Max
- Pre, Goal, Post and additional phases
- Students can view their fitness scores and enter their own Goal values
- Standards can be minimum values, maximum values or a range of values
- Standards can be viewed on screen or printed
- Fitness measurements can be marked as adapted scores, medical excuse or not tested
- **Fitness Reporting**
 - **Fitness Measurements Reports** – class reports, summaries by class, by teacher, by school and /or by district, historical reports by year
 - **Phase Comparison Reports** – utilize a wide variety of criteria to create comparison reports by class, by teacher, by school and /or district
 - **Student / Parent Fitness Report** – current year data, historical data for each year participating, comparison to fitness standards, letter/text customized by the customer with school logo included, can be made available in multiple languages
 - **Previous Score Report** – view previous fitness scores of current students

Cognitive Assessment Module

- Designed to be used in concert with Five for Life® curriculum or independently
- Ability to create custom assessments from question bank and create your own questions
- Assesses student understanding of fitness, health and nutrition concepts
- Students can access assessments from any internet enabled device
- Multiple choice and true/false questions are scored automatically
- Short answer and extended response questions can be viewed and scored easily
- View and print completed individual student test when taken online
- Ability to manually enter scores from hard copy assessments
- **Assessment Reporting**
 - **Item Analysis** – identify comprehension or deficiencies
 - **Summary Report** – view and print by class, by teacher and by assessment type
 - **View & Print Scores** – total points and percentage scores for each student's assessment
 - **Export to Spreadsheet Format** – for additional review and manipulation



FOCUSED FITNESS

Sensible Fitness and Health Programs for Today's Kids

Historical Data

- Historical data is available for teachers, students, parents and administrators
- Scores move with students in the system, even as they change schools in the district
- Ability to import data from other software systems

Administration

- Automatic class roster import and updates on your schedule
- Perform quality control to ensure accuracy of import
- Manual class roster updates as needed on request
- Administrative users can add, remove and maintain user accounts

Data Extraction Services

- Items available for de-identified raw data extraction and analysis are dependent on Modules purchased and can include:
 - Fitness Measurements
 - Cognitive Assessments
 - Behavior Logs
 - Rubrics
 - Surveys
- Administrative reports can be run for multiple school districts as needed by consortiums, researchers and evaluators

Security of Data

- Password protected login
- Access to class data is established on a per-school or per class basis
- WELNET® is backed up offsite, daily to ensure against loss of data
- Data security is ensured to meet FERPA (Family Educational Rights and Privacy Act) and HIPAA (Health Insurance Portability Accountability Act)
- Policies in place to ensure security of data including Security Audit Policy, Data Disposal Policy and Privacy Policy

WELNET® DS provides a district-wide solution to gather and retrieve longitudinal student health and fitness data in a simplified internet-based approach. Analyzing information in WELNET® DS helps students become aware of their behaviors and how the lifestyle choices they make can impact their



FOCUSED FITNESS

Sensible Fitness and Health Programs for Today's Kids

current and future health and fitness. Teachers can improve student progress, document student learning and exhibit student growth for goal setting and evaluation. It provides administrators with data confirmation of program impacts and changing needs.

WELNET® DS will assist in collecting and analyzing information information to improve the fitness and health of our youth.

EXHIBIT "C"

SCHEDULE OF DATA

TO BE COMPLETED BY VENDOR

[INSERT DETAILED DESCRIPTION OF DATA ELEMENTS HERE
NOTING REQUIRED AND OPTOINAL ELEMENTS]

See following page

Field Name	Required/Optional	Type	Max Length	Notes
Student Id	Required	Character	256	This should be unchanging year to year, it should not change if a student moves from one school to another, and it should not be reused after a student leaves the district.
Student Username	Optional	Character	256	If provided, this will be the username of the students when they login to WELNET®. If this is not provided, the student's username will be their Student Id.
Last Name	Required	Character	256	The last name of the student.
First Name	Required	Character	256	The first name of the student.
Middle Name	Optional	Character	256	The middle name of the student.
Email Address	Optional	Character	256	The email address of the student. This is only used by a student to reset their password. No other emails are ever sent to the students.
Date of Birth	Required	Character	6	Accepted formats include: mm/dd/yy, mm/dd/yyyy, yyyy-mm-dd, and many others
Gender	Required	Character	1	Accepted values include M, F, boy, girl, male, female
Student Password	Optional	Character	256	If included, this will be the password the student will use to login to WELNET®. When the password is supplied by the school district, the student cannot change their password.
Parent Password	Optional	Character	256	If included, this will be the password the student's parent will use to login to WELNET®
Parent Email	Optional	Character	unlimited	Comma separated list of email addresses, no limit to the number of addresses, max length of 256 characters per address
School	Required	Character	256	This is the name of the school.
Teacher	Required	Character	256	This is the name of the teacher. The preferred format is Last, First, however we can accept the Last Name and the First Name as two separate fields if it is easier. For middle and high schools, this is normally the name of the PE Teacher. For elementary schools, PE classes are not normally scheduled in the SIS, so this is the name of the homeroom teacher.
Teacher ID	Optional	Character	256	An optional unique id identifying the teacher - a teacher number.
Grade	Required	Character	10	The grade of the student.
Period	Optional	Character	256	The period of the class.
Class	Optional	Character	256	The name of the class, e.g. 9th Grade PE.
Section	Optional	Character	256	The section of the class.
Term	Optional	Character	256	The term of the class, e.g. Yearlong, YR, Semester 1, S1, etc.
A/B Day	Optional	Character	256	The A/B or block day designation of the class