

DATA PRIVACY ADDENDUM – NFHS NETWORK

This Data Privacy Addendum ("DPA") is entered into by and between Jefferson County Public Schools ("Customer") and 2080 Media, Inc. d/b/a PlayOn! Sports ("Company", and together with Customer, the "Parties" and each a "Party"). All capitalized terms not defined in this DPA shall have the meanings set forth in the underlying NFHS Network School Broadcast Program (Pixellot Use) Agreement and/or any related Order Forms (together, the "Agreement").

This DPA is an addendum to, and forms part of, the Agreement and sets out the terms that apply when Customer Personal Information (as defined below) is Processed by Company under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Information are Processed.

This DPA does not apply to Personal Information processed by Company in its role as a Controller of Personal Information obtained directly from end-users ("Company Controller Data"), including:

1. by browsing Company's websites and mobile applications,
2. by utilizing Company's underlying services,
3. by purchasing tickets, subscriptions, streaming events or other products from Company, or
4. otherwise by contacting Company or providing Personal Information directly to Company in a separate customer relationship.

Company Controller Data shall be Processed in accordance with the Company Privacy Policy located at <https://www.nfhsnetwork.com/privacypolicy>.

DATA PROCESSING TERMS:

1 Definitions

- 1.1 Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.
- 1.2 For the purposes of this DPA the following words and phrases shall have the following meanings:

"Consumer" means a natural person or resident or "data subject" as the term is understood under Data Protection Laws and Regulations.

"Controller" shall mean the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Information;

"Customer Personal Information" means the Personal Information of Consumers provided directly by Customer to Company in connection with the performance of the Services under the Agreement;

"Data Protection Laws and Regulations" means all applicable federal and state laws and regulations binding on a Party with respect to the Party's processing, protection, or privacy of the Personal Information, including where applicable, binding guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. Data Protection Laws and Regulations includes, but is not limited to, the California Consumer Privacy Act of 2018, as amended and supplemented by the California Privacy Rights Act of 2020, as may be further amended from time to time, and their implementing regulations ("CCPA");

"Services" has the meaning set forth in the Agreement; and

"Business Purpose," "Processing," "Processed," "Process," "Personal Information," "Sell," "Service Provider," "Share," "Subcontractor" shall have the same meaning as those terms in the CCPA or other Data Protection Laws and Regulations.

2 Processing of Customer Personal Information

2.1 Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Customer Personal Information as is necessary for providing the Services, Customer is the Controller, Company is the Service Provider.

2.2 Data Minimization. Customer recognizes and agrees that: (1) the Services generally do not involve substantial Processing of Customer Personal Information; and (2) Company generally does not expect to collect, store, or otherwise process Customer Personal Information in any substantial amount. Customer shall endeavor to, and shall train its personnel to, exercise all possible care in minimizing Company's access to or Processing of any Customer Personal Information to the extent solely and strictly necessary for the performance of the Services.

2.3 Customer's Processing of Customer Personal Information. Customer, as Controller, shall: (i) be responsible for ensuring that it has complied, and will continue to comply, with all applicable Data Protection Laws and Regulations; (ii) ensure it has, and will continue to have, the right to process, transfer, and/or provide access to, the Customer Personal Information to Company for Processing in accordance with the terms of the Agreement and this DPA; and (iii) have sole responsibility for the accuracy, quality, and legality of Customer Personal Information and the means by which Customer acquired Customer Personal Information.

2.4 Company's Processing of Customer Personal Information. Company shall treat Customer Personal Information as Confidential Information and shall Process Customer Personal Information on behalf of Customer as is necessary for providing the Services and only in accordance with Customer's documented instructions as set out in this DPA. Any Processing required outside of the scope of these instructions will require prior written agreement between the Parties. The Parties acknowledge and agree that Company's Processing of Customer Personal Information is as a Service Provider for a Business Purpose (i.e., performing services on behalf of Customer).

2.5 Data Protection Impact Assessments. Upon Customer's request and if required by applicable Data Protection Laws and Regulations, Company shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation to carry out a data protection impact assessment related to Customer's use of the Services.

3 Details of Data Processing.

3.1 Categories of Consumers and Customer Personal Information. The Consumers whose Customer Personal Information may be Processed by Company under the Agreement include Consumers acting in an employment capacity on behalf of the Customer to initiate and facilitate the Agreement. Customer Personal Information Processed in this context includes identification and contact information (name, email, title).

3.2 Retention Period. In connection with the termination or expiration of the Agreement for any reason, Company will cease any and all Processing of Customer Personal Information which is not strictly necessary to enable Company to comply with any obligations under this DPA or the Agreement. Upon Customer's request, Company will return to Customer and/or securely destroy all Customer Personal Information within 30 calendar days of the end of the services relating to the Processing or within 30 calendar days of Customer's request, except to the extent that applicable legal requirements require storage of the Customer Personal Information, in which case Company will (a) to the extent

legally permitted, inform Customer of the legal requirement and of the particular Customer Personal Information records that Company intends to retain, (b) not Process the Customer Personal Information for any purpose other than compliance with the applicable legal requirements, and (c) at the choice of Customer, return to Customer or securely destroy such Customer Personal Information as soon as practicable.

4 Rights of Consumers

- 4.1 **Consumer Request.** Company shall promptly notify Customer if Company receives a request from a Consumer to exercise the Consumer's rights, including to access, correct, obtain a portable copy, or delete Customer Personal Information as allowed by the CCPA or Data Protection Laws and Regulations (each such request being a "**Consumer Request**"). Taking into account the nature of the Processing, Company shall assist Customer by appropriate technical and organizational measures for the fulfillment of Customer's obligation to respond to a Consumer Request under CCPA or Data Protection Laws and Regulations. In addition, if requested by Customer, Company shall assist Customer in responding to such Consumer Request.

5 Company Personnel

- 5.1 **Confidentiality.** Company shall ensure that its personnel engaged in the Processing of Customer Personal Information are informed of the confidential nature of the Customer Personal Information, have received appropriate training on their responsibilities, and have executed written confidentiality agreements.

6 Subcontractors

- 6.1 **Use of subcontractors.** Customer acknowledges and agrees that: (i) Company's Affiliates may be retained as subcontractors, and (ii) Company and Company's Affiliates may engage third-party subcontractors in connection with the provision of the Services. If such subcontractors are engaged in the Processing of Customer Personal Information, Company shall ensure such subcontractors are informed of the confidential nature thereof and have executed written confidentiality terms.
- 6.2 **Liability.** Company shall be liable for its subcontractors to the same extent Company would be liable if performing the services of each subcontractor directly under the terms of this DPA.

7 Security

- 7.1 **Controls for the Protection of Customer Personal Information.** Company shall maintain reasonable and appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Personal Information), confidentiality and integrity of Customer Personal information in accordance with Appendix A Security Policy.
- 7.2 **Personnel.** Company shall take all reasonable steps to ensure the reliability of any Company personnel who may have access to, or are authorized to process, Customer Personal information. Company shall ensure that such Company personnel are bound by appropriate contractual confidentiality, data protection, and data security obligations in accordance with applicable Data Protection Laws and Regulations and this DPA.
- 7.3 **Compliance Monitoring.**

- 7.3.1 Upon Customer's reasonable request, Company shall make available to Customer all information in Company's possession necessary to demonstrate Company's compliance with its obligations under this DPA and Data Protection Laws and Regulations.
- 7.3.2 Upon written request, Customer may monitor Company's compliance with this DPA through regular assessments to be conducted in the form of a written questionnaire once per year.

8 CCPA Specific Provisions.

- 8.1 **Scope.** The following provisions apply to Customer Personal Information that is subject to the CCPA, or to any other Customer Personal Information to the extent required by other Data Protection Laws and Regulations. Company shall not:
 - 8.1.1 Sell or Share Customer Personal Information or any other similar concepts defined in Data Protection Laws and Regulations except to perform the Business Purposes specified in this DPA and the Agreement;
 - 8.1.2 Combine Customer Personal Information that Company receives from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a Consumer, except to perform the Business Purposes specified in this DPA and the Agreement;
 - 8.1.3 Retain, use, or disclose Customer Personal Information that it receives from, or on behalf of, Customer for any purpose, including any commercial purpose, other than the Business Purposes specified in this DPA, the Agreement, or as otherwise permitted by the CCPA or outside of the direct business relationship between Customer and Company.
- 8.2 **Notification.** Upon determination by Company that it can no longer comply with CCPA or any Data Protection Laws and Regulations, Company shall notify Customer without undue delay.
- 8.3 **Certification.** Company certifies that it understands the restrictions set forth in this DPA and the CCPA and shall comply with these restrictions.
- 8.4 **Remediation.** Upon notice, Customer reserves the right to take reasonable and appropriate steps to stop and remediate Company's unauthorized use of Customer Personal Information.

9 Customer Personal information Incident Management and Notification

- 9.1 Company shall notify Customer without undue delay, and no later than 72 hours, after becoming aware of a confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Information (a "**Customer Personal Information Incident**").
- 9.2 To assist Customer in relation to any personal data breach notifications Customer is required to make under the Data Protection Laws and Regulations, Company shall include in the notification such information about the Customer Personal Information Incident as is required by such Data Protection Laws and Regulations, to the extent that such information is reasonably available to Company and shall take all reasonable and necessary steps to remediate the cause of such Customer Personal Information Incident, to minimize further Customer Personal Information Incidents. Where and insofar as Company cannot provide all the information relevant to a Customer Personal Information Incident at the same time, it may provide such information in phases without undue further delay.

10 General Provisions

- 10.1 Except as amended by this DPA, the Agreement will remain in full force and effect.
- 10.2 If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.
- 10.3 Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.
- 10.4 This DPA will automatically terminate on the termination or expiry of the Agreement.
- 10.5 This DPA shall only become legally binding between Customer and Company when the Parties have executed below.

[Signature page follows]

The parties' authorized signatories have duly executed this DPA:

2080 MEDIA, INC.

[CUSTOMER]

By: David Graff
Name: David Graff
Title: CRO
Date: 07/24/2026

By: _____
Name: Dr. Brian Yearwood
Title: Superintendent
Date: _____

Appendix A Security Policy

This Security Policy ("**Security Policy**") outlines particular administrative, logical, technical and security requirements ("**Security Requirements**") that Company shall maintain to protect the availability, confidentiality and integrity of all Company systems, applications, and platforms ("**Company Network**"). Any capitalized terms used but not defined herein shall have the meaning set forth in the applicable DPA. In the event of any conflict between the terms of the DPA and this Security Policy, this Security Policy shall govern.

1. Access Controls

1.1. Authentication

Overview. Company requires authentication for access to all application pages on the Company Network, except for those intended to be public.

Secure Communication of Credentials. Company currently uses TLS-encrypted requests to transmit authentication credentials to the Company Network.

Password Management. Company has processes designed to enforce minimum password requirements for the Company Network. Company currently enforces the following requirements and security standards for end user passwords on the Company Network:

- Passwords must be a minimum of 8 characters in length and include a mix of uppercase and lowercase letters as well as numbers and symbols;
- Multiple logins with the wrong username or password will result in a locked account, which will be disabled for a period of time to help prevent a brute-force login, but not long enough to prevent legitimate users from being unable to use the application;
- Email-based password reset links are sent only to a user's pre-registered email address with a temporary link;
- Company rate limits multiple login attempts from the same email address; and
- Company prevents reuse of recently-used passwords.

Password Hashing. User account passwords stored on the Company Network are hashed with a random salt using industry-standard techniques.

Single Sign-On. In some instances, Security Assertion Markup Language (SAML) Single Sign-On (SSO) may be implemented through Company's SSO provider.

1.2. Session Management

Overview. Each time a user signs into the Company Network, the system assigns them a new, unique session identifier, currently consisting of 64 bytes of random data designed for protection against brute forcing.

Session Timeout. All sessions are designed to have a hard timeout. SSO sessions are configured with an inactivity timeout. There is an optional setting to terminate any sessions after 10 minutes of inactivity.

Sign Out. When signing out of the Company Network, the system is designed to delete the session cookie from the client and to invalidate the session identifier on Company servers.

2. Network and Transmission Controls

Company monitors and updates its communication technologies periodically with the goal of providing network security.

2.1. TLS and AES

Company encrypts all data at rest and in transit. Data is stored in AWS RDS and encrypted with custom keys from AWS KMS. All database connections use TLS. HSTS is used to ensure browsers' encryption of communication.

2.2. Network Security

Company regularly updates network architecture schema and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

2.3. Infrastructure Security

Company uses an Intrusion Detection System (IDS) and Endpoint Detection and Response (EDR), and other security monitoring tools on the production servers hosting the Company Network.

3. Data Confidentiality and Job Controls

3.1. Internal Access to Data

Access to customer data is restricted within Company to employees and contractors who have a need to know this information to perform their job function, for example, to provide customer support or to maintain infrastructure.

Company currently requires the use of SSO, strong passwords and/or 2-factor authentication for all employees to access production servers for the Company Network.

3.2. Job Controls

Company has implemented several employee job controls to help protect the information stored on the Company Network:

- All Company employees are required to sign confidentiality agreements prior to accessing Company's production systems;
- All Company employees are required to receive security and privacy training at time of hire, as well as quarterly security and/or privacy awareness training;
- Employee access to production systems that contain your data is logged and audited;
- Company employees are subject to disciplinary action, including but not limited to termination, if they are found to have abused their access to customer data; and
- Company employees are subject to background check prior to employment, where permitted by law.

4. Security In Engineering

4.1. Product Security Overview

The engineering process for the Company services follows industry-standard code development processes designed to ensure security at the product development and engineering levels. All changes to servers and infrastructure are implemented as code using industry standard tools and undergo the systems development lifecycle process as changes to the software.

4.2. Code Assessments

The software Company develops for the Company Network is continually monitored and tested using processes designed to proactively identify and remediate vulnerabilities. Company regularly conducts:

- Source code analysis designed to find common defects;
- Peer review of all code prior to being pushed to production;
- Manual source code analysis on security-sensitive areas of code; and
- Third-party application security assessments and penetration tests.

5. Availability Controls

5.1. Disaster Recovery

The infrastructure for the Company Network is designed to minimize service interruption due to hardware failure, natural disaster, or other catastrophes. Features include:

- **Cloud providers:** Company currently uses Amazon Web Company Network, which is trusted by thousands of enterprises to store and serve their data and services.
- **Data replication:** To help ensure availability in the event of a disaster, the cloud provider replicates data across multiple data centers.
- **Backups:** Company's cloud provider performs daily, weekly, and monthly backups of data stored on the Company Network.

5.2. Incident Response

Company has an incident response plan designed to promptly and systematically respond to security and availability incidents that may arise. The incident response plan is tested and refined on a regular basis.

6. Segregation Controls

6.1. Data Segregation

The Company Network is designed to logically separate each customers' data from that of other customers. Company's application logic is designed to enforce this segmentation by permitting each end user access only to accounts that the user has been granted access to.

6.2. User Roles

User roles specify different levels of permissions that the customer can use to manage the users on the Company Network account. Customer can invite users to customer's Company account without giving all team members the same levels of permissions.

7. Physical Security

Company uses a third party cloud platform (currently Amazon Web Company Network ("AWS")) to host its production systems for the Company Network. Access to AWS's data centers is limited to authorized

personnel only, as verified by biometric identity verification measures. Physical security measures for AWS data centers include: on-premises security guards, closed circuit video monitoring, and additional intrusion protection measures. Company relies on their third party attestations of their physical security. Within Company's physical office, Company employs a number of industry-standard physical security controls.

8. Patch and Vulnerability Management

Vulnerabilities meeting risk criteria defined by Company trigger alerts and are prioritized for remediation based on their potential impact to the Company Network. Upon becoming aware of such vulnerabilities, Company will use commercially reasonable efforts to address any vulnerabilities within a reasonable timeframe. Vulnerabilities which Company deems to be critical in nature will be remediated or mitigated within 30 days. Regardless of severity, Company remediates or mitigates all vulnerabilities within 90 days.



SCHOOL BROADCAST PROGRAM

Special Pixellot Term Renewal Agreement

Effective Date: _____

Jefferson County Public Schools
3332 Newburg Road
Louisville, KY 40218

This Special Pixellot Term Renewal Agreement (our "Agreement") will serve as confirmation of the renewal of Jefferson County Public Schools ("District") in the NFHS Network District Broadcast Program, powered by PlayOn! Sports, and will outline the terms and conditions of the renewal with 2080 Media, Inc. d/b/a PlayOn! Sports ("PlayOn"). Upon execution of the Agreement, District and PlayOn (collectively, the "Parties") are subject to the terms of the Agreement set forth herein.

Definitions:

"Prior Agreement" means the one or more agreements under which District received Pixellot automated camera systems (collectively, the "Prior Agreements").

"Leased Pixellots" means the Pixellot automated camera systems that District leased from PlayOn under the Prior Agreements. Leased Pixellots are the property of PlayOn.

"Pixellot Systems" means the total number of Purchased Pixellots and Leased Pixellots.

Upon the Effective Date, any Prior Agreements are no longer in effect. District acknowledges and agrees that all Pixellot Systems shall be governed by the terms of the Agreement as set forth herein.

PlayOn provides the following additional software and services:

- A branded District video portal on www.nfhsnetwork.com
- PlayOn proprietary software (NFHS Network Console) for the complete management of District-based events including scheduling, event information, and event availability. The cost of the annual software license for the PlayOn Software (Console) is waived as part of the Agreement.
- E-commerce platform for customer registration, payment processing and customer service to support the sale of subscriptions to watch District and all other NFHS Network events ("Consumer Subscription Plan")
- All back-end technology systems needed to support event distribution via streaming consistent with PlayOn system requirements through the NFHS Network web portal
- Standard on-call customer success, customer support, training, software updates, software support, and software licenses.

In consideration of a one-time fee of zero dollars (\$0 ("One-Time Fee"), PlayOn will provide district with access to sixty (60) units of hardware and software ("Pixellot Systems") for school use during the term of this Agreement in the following district schools (but PlayOn will retain title to such items), each of which includes:

- | | |
|---------------------------|-------------------------------------|
| 1. Atherton High School | 13. Jeffersontown High School |
| 2. Ballard High School | 14. Male High School |
| 3. Brown High School | 15. Manual High School |
| 4. Butler High School | 16. Moore High School |
| 5. Central High School | 17. Pleasure Ridge Park High School |
| 6. Doss High School | 18. Seneca High School |
| 7. Eastern High School | 19. Shawnee High School |
| 8. Fairdale High School | 20. Southern High School |
| 9. Fern Creek High School | 21. Valley High School |
| 10. Grace James Academy | 22. Dubois High School |
| 11. Iroquois High School | 23. Waggener High School |
| 12. Newcomer High School | 24. Western High School |

Broadcast Rights and Event Content:

Regular Season Event Broadcasts.

District agrees to live broadcast all regular season sports events at all competition levels in the venue where the Pixellot Systems are installed (i.e., Varsity, Junior Varsity, etc.). District has the right to determine on-demand availability of regular season events through



SCHOOL BROADCAST PROGRAM

"blackout windows." District will not permit any third party to stream any regular season sports events that would be deemed competitive with PlayOn's activities; provided that District may allow student-led groups to live broadcast regular season sports events ("District Co-Broadcasts") as part of a broadcast media curriculum program and any other types of terrestrial radio, internet audio, or existing District broadcasts in place as of the Effective Date. For the sake of clarity, events selected by District or District Co-Broadcasts will also be broadcasted on the NFHS Network via the Pixellot Systems.

Television Broadcasts. District may allow (at its discretion) third party local television coverage to broadcast regular season events at a District without violating the Agreement. For the sake of clarity, District shall also broadcast via the Pixellot Systems on the NFHS Network any regular season event that is broadcast on linear television by a third party.

Postseason Event Broadcasts. District agrees that the Pixellot Systems will be used to broadcast all State Postseason events via the Pixellot System installed in the venue where the event takes place; provided that State Association is a participating member of the NFHS Network ("NFHS Network State"). State Association rights fees for State Postseason events broadcast via the Pixellot System at District venues will be waived in NFHS Network States. For Districts located in non-NFHS Network States, all broadcasting of State Postseason events must be done within State Association media policies and District is solely required to obtain required permissions and pay any rights fees to the State Association.

Practices. District may use the Pixellot Systems to schedule and record practices for internal use by District. District must manually schedule all practice sessions and events will be marked as "private" and not available for viewing by consumers.

Content Ownership, License, Syndication and Approvals. District hereby grants PlayOn an exclusive, worldwide, fully-paid-up, royalty-free, sub-licensable (directly or through multiple tiers), transferrable and irrevocable license to reproduce, perform, transform and distribute the content recorded via the Pixellot Systems (the "Content") in any medium (the "Content License"). The Content License is exclusive, except that the District has the right to download District-produced events and upload the Content into a game-film-analysis platform for use by coaches, provided that the Content is not generally available to consumers. Subject to the Content License, the Content is the exclusive property of the District and the District reserves all rights therein. Notwithstanding the foregoing, this Content License does not extend to any use that is false, defamatory, or that presents a student athlete or the District in a negative light. These exceptions to the License shall not extend to any game footage in its original state.

The Content License includes the right to syndicate the Content, in-part or in-whole, to other distribution platforms. Existing digital sponsorship inventory remains in the Content through all derivative works that incorporate the full-length event.

District shall be solely responsible to secure any and all releases, consents, waivers and other necessary rights from any third parties (including students and, to the extent required by law, their guardians) and complying with all applicable laws, including those regarding collection and distribution of the Content. District agrees that all Content will be suitable for a general viewing audience and will not violate or infringe the rights of any party. At the written request of District, PlayOn will remove District produced events on the District video portal. Parties agree that Pixellot System will not be turned on except for scheduled events and required system maintenance.

Consumer Subscription Platform. All sports events, live and on-demand, require consumers to purchase a subscription pass to be viewed. Non-sports events are set by default to be free for viewers. At District's discretion, District may charge a subscription fee to view non-sports events.

PlayOn retains the right to modify subscription plan offerings, pricing structure, and, during the Term, on-demand event availability. PlayOn will notify District in writing of any such modifications.

District-sold Sponsorships. District may include sponsorship elements within the broadcast of District events in its District video portals. District keeps 100% of all sponsorship sales made by District from local sponsors.

Network Advertising. PlayOn may advertise on any District video portal and within any District broadcast using pre-roll video, video mid-roll, or overlay ads that appear on the video screen. PlayOn ads will conform to the then-current *NFHS Network Commercial Materials Guidelines* (the "Guidelines"), a current copy of which is attached as Exhibit B; provided that District shall have the right in its sole discretion to limit or prohibit any advertiser, or any specific advertisement advertised on the District video portal, that is inconsistent with District standards for appropriateness for viewing by the District district's student population.

Third Party Relationships. Any third-party relationships District develops for the purpose of selling advertising, collecting billings or any other such related activity, are the sole right and responsibility of District. PlayOn assumes no responsibility whatsoever for (and shall have no liability for) any third-party relationships District enters into.

Data Privacy. District acknowledges that PlayOn will not have access to any "student information," "directory information," "personally-identifiable information," student records," "student-generated content" or "education records" (each as defined by the Family Education Rights and Privacy Act of 1974 ("FERPA") and its implementing regulations, other than, to the extent included in the Content as applicable: (a) student images; (b) student names; and (c) any other information provided by District in the format of audio commentary (the "Included Data"). District acknowledges that the Included Data is only included in the Content to the extent permitted by the District and to the extent publicly broadcasted at the event contained within the Content. PlayOn shall not have access to any other information regarding any District students and does not store any information regarding District students that is not Included Content meant for public consumption through the NFHS Network and other customer-facing applications. PlayOn shall be responsible to comply with all applicable laws, including but not limited to FERPA and any state-specific laws regarding Included Data and the collection, storage and distribution thereof, but subject to District's responsibilities under "Content Ownership, License, Syndication and Approvals" set forth above. In furtherance of the foregoing, PlayOn will maintain security procedures and practices designed to protect the Included Data



SCHOOL BROADCAST PROGRAM

from the unauthorized access, destruction, use, modification or disclosure that comply with FERPA and any state-specific laws, and will notify the District following PlayOn's becoming aware of any such unauthorized access, destruction, use, modification or disclosure of Included Data. PlayOn will not use the Included Content for any purpose other than as contemplated by this Agreement and PlayOn will, upon District's written request at any time, permanently delete any Included Content.

To the extent District requires that PlayOn execute any amendment or addendum to this Agreement governing the rights and obligations of Included Data, the Parties agree that this provision shall supersede such amendment or addendum and shall contain the sole obligations of PlayOn with respect to Included Data.

Consent to Receive Electronic Communications. During the Term, PlayOn will send updates and alerts related to the Pixellot Systems via SMS text message (the "Notifications") to the individuals listed on the Primary Contact Information chart attached hereto and any other employee or agent of District that District elects to receive the Notifications (together, the "Notification Contacts"). District hereby represents and warrants to PlayOn that the District and each Notification Contact (i) has read PlayOn's privacy policy (found at <https://www.nfhsnetwork.com/privacypolicy>) and understands the privacy policy, the types of information being collected and PlayOn's use of the information being collected and (ii) expressly consents to receive the Notifications.

Terms and Conditions

1. **Term of Contract.** This Agreement is effective as of the Effective Date and continues for one (1) complete District school years, beginning on the August 1 that follows the Effective Date (the "Renewal Term") unless earlier terminated as provided herein.

After the Renewal Term, the Agreement will automatically renew for successive four (4)- one year periods (each, a "Successive Term", and together with the Renewal Term, the "Term") unless terminated as provided herein. District has the right to terminate this Agreement at the end of the Renewal Term or any Successive Term by giving written notice of non-renewal to PlayOn a minimum of sixty (60) days before the end of the Renewal Term or Successive Term, as applicable, whereupon the Agreement shall terminate on the last day of the Renewal Term or the then-current Successive Term, as the case may be.

PlayOn may terminate this Agreement and remove the Leased Pixellots immediately if District has breached any provision of this Agreement and failed to cure such breach within sixty (60) days of PlayOn's delivery to District of written notice of the breach; provided that District will take down all equipment and package it appropriately in PlayOn-provided shipping containers. In the event that PlayOn breaches any provision of this agreement and fails to cure within sixty (60) days, District has the right to terminate the Agreement and PlayOn will remove the Leased Pixellots at its own expense.

2. **Internet Connectivity.** District must provide sufficient hardline Internet connectivity and the required network configurations (provided in Exhibit A) for each Pixellot System to allow live broadcasts. PlayOn will provide the point-to-point wireless Internet base station ("Point to Point") when needed to deliver hardline Internet connectivity to Pixellot Systems installed in outdoor venues; provided that PlayOn is able to select the make and model of the Point to Point system. In the event that District requests, or requires, a specific Point to Point system that is different from what is provided by PlayOn, then District must provide and install the Point to Point system at its own expense.
3. **Software License.** During the Term of this Agreement, PlayOn grants District a non-exclusive, non-transferable limited license to use the Software to enable the broadcast services under this Agreement. The "Software" consists of the proprietary software of PlayOn used to provide the broadcast services under this Agreement as well as the third-party software included with the Pixellot Systems and any backend software or services required to use the system. The Software may be used solely to schedule, capture, produce, encode, and record Content from District events for distribution to viewers solely on the NFHS Network. District shall have no other rights to the Software and expressly agrees that it shall not copy, reverse engineer, modify, disassemble or decompile any portion of the Software, or use the Software to broadcast events anywhere other than District pages on the NFHS Network video portal (www.nfhsnetwork.com). District agrees that PlayOn or its licensors shall retain any and all right, title, and interest in and to the Software and other intellectual property provided by or created by PlayOn (including, but not limited to, all patent, trade secret, copyright, and trademark rights). Except as otherwise provided herein, District agrees not to reproduce the Software or PlayOn's intellectual property. District acknowledges that the Pixellot Systems include embedded software from Pixellot that is subject to additional end-user license agreement terms ("EULA") and District agrees to comply with all such terms. The Pixellot EULA will be provided at the District's request.
4. **Revenue Share.** District will receive twenty percent (20%) of the Revenue ("Revenue Share") for Monthly subscription passes attributed to District's Pixellot System-produced content.

PlayOn will offer "discounted" Annual (12 month) subscription passes for sale on District event pages and on custom District landing pages, meaning the one-time cost of the subscription pass is less than the cost of the Monthly pass times the number of months in the duration of the Annual subscription pass. Annual subscription passes will have a base cost ("Annual Base Cost") and a price point ("Annual Price"), both set by PlayOn. Starting in Year 1, District will receive one hundred percent (100%) of the difference between the Annual Price and the Annual Base Cost.

5. **Administration of Funds.** PlayOn will manage the collection and accounting of all funds received, including the management of refunds. If District produces regular season content on an alternative streaming platform in violation of this Agreement, PlayOn reserves the right to withhold any Revenue Share attributed to District. PlayOn will calculate the funds to be disbursed to District on a quarterly basis on the following dates: October 31st, January 31st, April 30th, and July 31st. Funds will be disbursed to District within 30 days of these dates. Detailed records can be provided for auditing purposes upon request. District must earn a minimum of \$50 in aggregate Revenue Share proceeds within a District year to receive a check.
6. **Ownership of Leased Pixellots.** District may not move a Leased Pixellot from where it was installed without the express written consent of PlayOn. Leased Pixellots will remain PlayOn's property and PlayOn may remove the Leased Pixellots from District if this Agreement



terminates for any reason or if District fails, in any nine (9) month period, to create any Content via a Leased Pixellot for distribution on the NFHS Network. District shall cooperate with PlayOn to facilitate this removal and shall grant PlayOn any required physical access to the Leased Pixellots.

7. **Maintenance of Units.** PlayOn is responsible for the general health and welfare of the Pixellot Systems (including all Purchased Pixellots from any Prior Agreements) and will perform online system maintenance of all Software. PlayOn will handle all warranty claims on the equipment with the manufacturer and will provide District with proper containers for any equipment that needs to be returned to PlayOn for service. PlayOn will upgrade or replace any non-functioning Pixellot Systems (including all Purchased Pixellots) during the Renewal Term on an as-needed basis.

For the sake of clarity, this Paragraph 11 shall apply to all Pixellot Systems, which includes Purchased Pixellots and Leased Pixellots. Any Purchased Pixellot or Leased Pixellot that is replaced pursuant to this Paragraph 11 shall be deemed a Leased Pixellot for the purposes of this Agreement.

8. **Providing of Sports Schedules.** District is required, prior to 60 days before the start of a sport season, to provide PlayOn the game schedules (in a mutually acceptable format) for all teams in all sports that occur in the venue where the Pixellot System is installed. PlayOn will be responsible for the initial data entry of all game schedules in the event that District does not elect to do so. In event of a known change of schedule to an event, District will make the required changes.

If District's game schedules are accessible via a third-party platform (e.g. Arbitrator, rDistrictToday, etc.), District agrees that PlayOn may collect District's game schedule information directly from that third-party platform, to be used for the sole purpose of scheduling automated event broadcasts on the NFHS Network through District's Pixellot System(s). District will facilitate PlayOn's access to District's game schedule on any such third-party platform.

9. **Marketing.** District agrees that PlayOn may market District's events on third party platforms or websites (e.g. Arbitrator, rDistrictToday, MaxPreps, etc.). Event marketing includes, but is not limited to, URL links and display ads.
10. **Indemnification.** PlayOn (the "Indemnifying Party") shall indemnify, hold harmless, and, at the request of District, defend the District (the "Indemnified Party") from and against any and all losses, liabilities, costs, and expenses including reasonable attorney's fees, in connection with claims brought by a third party against the Indemnified Party established by judgment or alternative resolution award, to the extent arising from (a) any violation of applicable law by the indemnifying party or its employee, agent, or other representative; (b) the gross negligence or willful misconduct in the performance of obligations hereunder by the indemnifying party or any employee, agent, or other representative of the indemnifying party.
11. **Indemnification for IP Infringement.** PlayOn shall indemnify District against any third-party claim that District's use of the Pixellot Systems infringes the intellectual property rights of a third party with respect to such Pixellot Systems; provided that, PlayOn shall have no obligation under this section with respect to any claim based upon or arising from: (a) modification of the Pixellot Systems in any manner not expressly permitted by PlayOn; (b) any use of the Pixellot Systems outside the scope of the license granted in, or contrary to, the provisions of, this Agreement or the EULA; (c) the combination of the Pixellot Systems with any other service or product not authorized by PlayOn or Pixellot; or (d) broadcasting the Content without a license, right or title to do so.
12. **WARRANTY DISCLAIMER; LIMITATION OF LIABILITY.** THE SERVICES AND SOFTWARE PROVIDED BY PLAYON ARE PROVIDED "AS IS." PLAYON MAKES NO WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE AND SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR ANY INDIRECT DAMAGES, INCLUDING CONSEQUENTIAL, SPECIAL, OR INCIDENTAL DAMAGES WHATSOEVER ARISING FROM OR IN ANY WAY RELATED TO THIS AGREEMENT OR THE RIGHTS OR OBLIGATIONS OF THE PARTIES HEREUNDER WHETHER OR NOT A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND WHETHER BASED ON A BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE. IN ADDITION, AND NOTWITHSTANDING ANY OTHER PROVISION IN THE AGREEMENT, PLAYON'S MAXIMUM LIABILITY (FOR ALL CLAIMS IN THE AGGREGATE) TO DISTRICT UNDER OR IN CONNECTION WITH THIS AGREEMENT SHALL NOT EXCEED THE AMOUNTS PAID TO DISTRICT UNDER THIS AGREEMENT. THE LIMITATION IN THE IMMEDIATELY PRECEDING SENTENCE DOES NOT APPLY TO (I) PLAYON'S OR ITS PERSONNEL'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT RESULTING IN PROPERTY DAMAGE, PERSONAL INJURY OR DEATH; OR (II) PLAYON'S OBLIGATION TO INDEMNIFY DISTRICT FOR THIRD PARTY INTELLECTUAL PROPERTY INFRINGEMENT CLAIMS.
13. **Relationship of the Parties.** Each Party shall have the status of an independent contractor for purposes of this Agreement. This Agreement is not intended to and will not create or otherwise recognize a joint venture, partnership, or formal business association or organization of any kind between the parties, and the rights and obligations of the parties shall only be those expressly set forth in this Agreement.
14. **Assignment.** This Agreement may not be assigned by either Party without the prior consent of the non-assigning Party.
15. **Entire Agreement; Modification.** This Agreement constitutes the entire understanding between the parties. It supersedes and replaces any and all previous representations, understandings, and agreements, written or oral, relating to the subject matter. There shall be no oral alteration or modification of this Agreement; the Agreement and its terms may not be modified or changed except in writing, approved and signed by both Parties.
16. **E-Verify.** PlayOn acknowledges that immigration laws require it to register and participate with the E-Verify program (employment verification program administered by the United States Department of Homeland Security and the Social Security Administration or any successor program).



SCHOOL BROADCAST PROGRAM

17. **Proof of Insurance.** During the Term, PlayOn shall maintain, and (upon District's written request) provide evidence of, commercial general liability, statutory workers' compensation insurances, and such public liability insurance as is reasonably necessary to protect against claims, losses or judgments that might be occasioned by the negligent acts or omissions of PlayOn, its employees or agents. The general liability insurance shall be at least in the amount of \$1,000,000 per incident and a \$2,000,000 aggregate.
18. **Governing Law and Venue.** This Agreement shall be interpreted in accordance with the substantive and procedural laws of the State in which the District resides. Any action at law or judicial proceeding instituted for the enforcement of this Agreement shall be instituted only in the state courts of the State and county in which the District resides.
19. **Counterparts.** This Agreement may be executed in counterparts (including by way of facsimile, PDF or other electronic format), each of which shall be deemed an original but all of which together shall constitute one and the same instrument.
20. **Waiver.** The failure of either Party to insist upon strict performance of any of the provisions of this Agreement or to exercise any rights or remedies provided by this Agreement, or either party's delay in the exercise of any such rights or remedies, shall not release the other Party from any of its responsibilities or obligations imposed by law or by this Agreement and shall not be deemed a waiver of any right of such Party to insist upon strict performance of this Agreement.
21. **Compliance with Applicable Laws; Sovereign Immunity.** Each Party shall comply with all applicable laws applicable to it with respect to the services being provided under this Agreement, whether or not specifically referenced in this Agreement. Nothing in this Agreement shall be deemed to waive any sovereign immunity, if any, for which the District may benefit.

[Signatures on Next Page]



SCHOOL BROADCAST PROGRAM

Signed:

Date: 07/24/2026

David Greiff CRO
PlayOn! Sports

Accepted by District:

Signature: _____

Name: _____

Title: _____

Email: _____

District: _____

Primary Contact: _____

Email: _____

Mobile Number: _____

Bookkeeper: _____

Email: _____

Phone Number: _____

IT/Network Contact: _____

Email: _____

Phone Number: _____

Facilities Contact: _____

Email: _____

Phone Number: _____

Subscription Revenue Check Made Out to: _____



SCHOOL BROADCAST PROGRAM

EXHIBIT A

NETWORK CONFIGURATION REQUIREMENTS

For the most up-to-date Pixelot streaming requirements, go to support.nphsnetwork.com and search for "Pixelot Streaming Requirements."

We highly recommend adding the VPU (Pixelot computer) to a separate **VLAN** or a **DMZ** and assigning a static IP address.

VPU's use Google Public DNS &&B.B as the preferred server. Please use your internal DNS as the alternate. We also ask that Gateway SSL Decryption is bypassed and any Internet Sleep Schedules are disabled.

No inbound firewall rules are required as all connections are outbound. Inbound traffic will still be present, but only after an outbound connection is established. No services will ever connect directly to the host. To publish video and manage the server, the following ports must be open for outbound connections to all IPs:

Port #	Protocol	Purpose	Application
443*	TCP required UDP optional	Remote Management/video streaming	https, agent
123*	TCP	Clock synchronization	NTP-clock sync
2088*	UDP	Video streaming backup	ZIXI broadcaster
5672*	TCP+UDP	Graphics, Watermarks, etc.	Scoreboard Graphics Generation
5678*	TCP+UDP	Backend Zixi broadcasts	ZIXI broadcaster

The following ports are **NOT** required to broadcast, but are **highly recommended** for keeping Sportcast (scoreboard integration device) software up to date:

1402	TCP	Sportcast cloud connect
1403	TCP	Sportcast remote support
1935	TCP	Remote Graphics support

In addition, please whitelist the **REQUIRED** domains in any active content filters below:

- *.nphsnetwork.com - Communication to scheduling services
- *.pixelot.stream - Communication to streaming services
- *.pixelot.tv - Communication to streaming services
- *.video.google.com - Streaming configuration
- *.geotrust.com - Certificate verification
- *.loginin.com - Remote control for troubleshooting
- *.cloudfront.net - Access to application updates
- *.sportcast.net - Scoreboard control
- *.app.singular.live - Scoreboard graphics

Network Speed Requirements

We recommend an upload speed of at least 10 Mbps. As a reminder, the Pixelot system must be plugged into a ethernet port (not wi-fi or cellular data). For more information about establishing a stable Internet connection, please click [here](#).

General Guidelines

- **DO NOT** add any additional user accounts or change any user account settings
 - DO NOT change the password
 - DO NOT add the user to the District's domain
 - Adding/changing user account information affects the system's ability to automatically login after a reboot, which may result in events not broadcasting
 - DO NOT add the computer to the District domain
- **DO NOT** change firewall settings (or add additional firewall/antivirus software)
 - Antivirus software consumes CPU resources and can disrupt network traffic
- **DO NOT** make the computer inaccessible
 - Make sure you can access the machine if necessary
- **DO NOT** leave a monitor, keyboard, mouse, or any other external device plugged in
 - Leaving these plugged in may affect our Support team's ability to remotely access the system for troubleshooting
- **DO NOT** use the computer for anything unless specifically directed by NPHS Network Support

Video Stream/Data Transmission

1. All video data is transferred from Pixelot to the NPHS Network Servers using Real-Time Messaging Protocol (RTMP)
2. The NPHS Network Servers are all hosted using Amazon Web Services (AWS) in the North Virginia (US East) Data Centers
3. Once received by the NPHS Network, the video data is transcoded using automated servers (no human involvement), and then stored in the AWS S3 Storage Buckets (again hosted on AWS North Virginia)
4. The video is distributed to consumers using HTTP Live Streaming (HLS) using the AWS CloudFront Content Distribution Network



EXHIBIT B

NFHS NETWORK COMMERCIAL MATERIALS GUIDELINES

Advertising that shall be false, misleading, deceptive, offensive or in poor taste shall be subject to rejection. All advertisements must comply with the applicable laws, rules and regulations of the state associations and/or District Districts that govern the applicable broadcast.

Without limiting the generality of the foregoing, certain categories of advertisements will not be accepted without prior consent, which such consent may be withheld for any reason whatsoever. These categories include the following:

1. Advocacy Advertisements. An advocacy advertisement is any advertisement that advocates a political, religious or controversial public position.
2. Cigarettes or Tobacco Advertisements.
3. Betting or Gambling Advertisements.
4. Firearms Advertisements.
5. 900 Phone Number Advertisements.
6. Contraceptive Advertisements.
7. Tattoo Parlor and Body Piercing Advertisements.
8. "NC-17" Rated Movie Advertisements.
9. Adult Entertainment Advertisements.
10. "R" Rated Movie Advertisements.
11. "M" Rated Electronic (computer or video) Games Advertisements.
12. Hard Liquor Advertisements.
13. Beer, Wine, or other Alcoholic Beverage Advertisements
14. "High Risk" Investments (e.g., commodities, options, foreign exchange) Advertisements.
15. "High Risk" Business Opportunities (e.g., "get rich quick" schemes and business opportunities) Advertisements.
16. "High Risk" Health Offerings.