FIFTH AMENDMENT
to the
SCHOOL RESOURCE OFFICER PROGRAM AGREEMENT

This Agreement ("Agreement") made effective as of _____, by and between the OLDHAM COUNTY BOARD OF EDUCATION, (hereinafter referred to as the "School District"), the OLDHAM COUNTY FISCAL COURT, and the OLDHAM COUNTY POLICE DEPARTMENT (hereinafter referred to as the "OCPD").

WITNESSETH:

WHEREAS, the OCPD and the School District entered into a School Resource Officer Program Agreement effective July 1, 2021 to provide School Resource Officers to the School District; and

WHEREAS, ARTICLE XII of the Agreement allows the parties to make modifications to the Agreement in writing; and

WHEREAS, the parties have the desire to expand the scope of information sharing to include OCPD Detectives for the purpose of enhancing student safety and streamlining emergency response;

NOW, THEREFORE, in consideration of the mutual promises and covenants herein contained, the School District and the OCPD hereby agree as follows:

ARTICLE VI
Information Sharing

Access to student education records is governed by the Family Educational Rights and Privacy Act ("FERPA") 34 CFR §99.

A. Directory Information. In accordance with OCBE Policy 09.14, the School District may provide Directory Information to law enforcement upon request for students who have not opted out. However, for the purposes of active safety and investigative duties, the digital access granted in Section E of this Article shall take precedence for Authorized Personnel.

B. Personally Identifiable Information (PII). Other than Directory Information, PII shall only be released to law enforcement with parental consent, a subpoena, or a court order, unless the officer is acting as a "School Official" as defined in Section E of this Agreement. The School District hereby designates authorized SROs and Detectives as School Officials with a legitimate educational interest for the limited demographic fields listed in Section E(1).

C. Video Recording. The School District maintains a system of video cameras and recording devices to increase safety and security at its schools and other locations. It is the School District's intent that the video recording system be used for investigative purposes, rather than surveillance. Access to the video recording system will be granted to the SRO for non-emergency investigative purposes in accordance with the provisions of FERPA if the recording depicts one or more identifiable students. In an emergency, the School District will provide the SRO and Oldham County Central Dispatch with unlimited access to recorded video or live feed if it is necessary to protect the health or safety of the students or other individuals.

D. Search and Seizure. Searches conducted by the School District will be performed in accordance with OCBE Policy 09.436. The SRO will conduct searches in conformance with state and federal laws, and OCPD policies. The SRO shall not ask the School District to search a student's person, school locker, personal belongings, electronic devices, or vehicle in an effort to circumvent the student's legal rights. Searches may include use of metal detectors, trained dogs, or breathalyzer instruments when appropriate.

E. **Access to Student Demographic Data**

1. **Grant of Access:** The School District shall provide authorized OCPD School Resource Officers (SROs) and Detectives (collectively, "Authorized Personnel) with individual secure logins to the Student Information System. Access shall be strictly limited to data fields as defined in APPENDIX I.
2. **Designation as School Officials:** For the purposes of this Agreement and in accordance with 34 CFR §99.31(a)(1)(i)(B), Authorized Personnel granted such access are designated as "School Officials" with a "legitimate educational interest." This interest is defined as the need to access student location and family contact information to maintain school safety, respond to emergencies, or conduct active investigations involving the welfare of the student body. A legitimate educational interest does not include the use of District data for general law enforcement purposes, or any investigation of a student or family member that is wholly unrelated to the safety, security, or operations of the School District.
3. **Direct Control and Use Limitation:** The OCPD agrees that Authorized Personnel utilizing these logins are under the "direct control" of the School District regarding the use and maintenance of education records. Information obtained through this access shall not be disclosed to any third party without parental consent or a court order, except as provided by law.
4. **Audit and Security:** The OCPD shall provide the School District's Director of Student Services and Director of Technology with a specific roster of SROs and Detectives authorized for login access. The School District reserves the right to audit access logs at any time.
    a. **Suspension of Access:** If the School District identifies a potential unauthorized use of a login or data, the District may immediately suspend that specific user's access pending an investigation.

b. **Joint Investigation:** In the event of a suspension, the District's Director of Student Services and the OCPD Chief (or designee) shall meet within five (5) business days to review the audit logs and the nature of the access.
c. **Determination and Discipline:** If the use is found to be a legitimate mistake or a technical error, access may be restored a the District's discretion.
    i. If the use is found to be a violation of FERPA or this Agreement, access for that individual shall be permanently revoked.
    ii. Any internal personnel discipline resulting from the misuse of data shall remain the sole responsibility and discretion of the OCPD in accordance with their department policies.
d. **Appeals:** The OCPD Chief may appeal a permanent revocation of a user's access to the School District Superintendent, whose decision shall be final regarding access to the District systems.

5. **Training Requirements:** Prior to receiving login credentials, each Authorized Personnel must certify they have received training on FERPA, and the privacy provisions outlined in this Agreement.

F. **Data Security and Breach Notification (KRS 61.931-61.934)**

1. **Independent Compliance and Stewardship:** The OCPD acknowledges that it is a public agency independently bound by the security and breach investigation requirements of KRS 61.931 to 61.934. Notwithstanding the OCPD's independent legal obligations, the parties agree that the School District is the legal custodian of all Student Education Records accessed via the provided logins, and the School District retains ultimate authority over the protection of these records.
2. **Notification of Security Breach:** In the event OCPD determines that a "security breach" (as defined in KRS 61.931) has occurred involving Student Education Records or district login credentials, the OCPD shall notify the School District's Director of Technology and Director of Student Services within seventy-two (72) hours of such determination.
3. **Cooperation in Mandated Reporting:** Following a breach, the OCPD shall provide the School District with all information necessary to fulfill its mandatory reporting obligations to the Kentucky Commissioner of Education, the Office of the Attorney General and the Auditor of Public Accounts.

G. **Termination of Access and Credential Management**

1. **Immediate Revocation:** The OCPD shall notify the School District's Director of Technology and Director of Student Services in writing within twenty-four (24) hours when any Authorized Personnel with login access:
    a. Leaves the employment of the OCPD;
    b. Is transferred out of the SRO program or the Detective investigative unit; or
    c. No longer requires access to student data to perform their official duties.
2. **District Action:** Upon receipt of such notice, or upon the District's own determination that an individual no longer requires access, the District shall immediately deactivate the associated login credentials.

3. **Annual Audit:** On or before July 1 of each year, the OCPD shall provide a certified list of all personnel currently holding active logins to ensure only authorized individuals maintain access.

IN WITNESS WHEREOF, the parties have caused this Agreement to be signed by their duly authorized officers.

OLDHAM COUNTY FISCAL COURT

_____ _____

David Voegele, Judge Executive *Date*

OLDHAM COUNTY POLICE DEPARTMENT

_____ _____

Greg Smith, Chief of Police *Date*

OLDHAM COUNTY BOARD OF EDUCATION

_____ _____

Carly Clem, Chairperson *Date*

_____ _____

Claudette Herald, Secretary/Superintendent *Date*

APPENDIX I: Authorized Personnel Data Access Mapping

Purpose: This Appendix defines the specific data elements within the School District's Student Information System (SIS) accessible to Authorized Personnel (SROs and Detectives) designated as "School Officials" under Article VI of the School Resource Officer Program Agreement.

1. **Authorized Demographic Data Fields**

Access is restricted to a "View-Only" profile. Authorized Personnel shall have access to the following specific data points only:

Data Category	Specific SIS Fields / Elements	Justification for Access
Student Profile	Legal Name Nickname Date of Birth Grade Level Current Enrollment Status Student Photo	Identification of students during active safety incidents or investigations.
Enrollment History	List of all schools attended within the District and dates of enrollment.	Establishing student location history and identifying potential peer associations.
Household / Address	Primary Physical Address Secondary / Mailing Address	Emergency response, welfare checks and service of legal processing.
Parent & Guardian	Legal Name of Guardians Relationship to Student Primary Phone Number Secondary Phone Number Email Address	Immediate notification of parents/guardians during emergencies or legal interactions.
Sibling Links	Names of siblings currently enrolled in the District and their assigned school locations.	Coordinating family reunification during crises or identifying household members.

2. **Prohibited Data Fields (Strictly Excluded)**

For the avoidance of doubt, the following modules and data points are **NOT** accessible to Authorized Personnel via the provided login:

- **Academic Records:** Grades, GPA, transcripts and teacher comments.
- **Attendance Records:** Detailed daily/period attendance or check-in/out logs (unless requested separately for a specific investigation).
- **Behavior/Discipline:** Disciplinary referrals, suspension history, or behavioral intervention plans.
- **Special Education:** IEP/504 status, disability categories, and related service records.
- **Health Records:** Immunizations, medications, and physical/mental health conditions.

3. **Technical Oversight**

- **Credential Source:** Credentials shall be issued and managed solely by the District SIS Data Manager.
- **Audit Frequency:** The SIS Data Manager shall perform a random audit of access logs at least once per semester to ensure access aligns with the "Legitimate Educational Interest" defined in Article VI(E)(2).