Inter-Agency Data-Sharing Agreement

North Thurston Public Schools (NTPS) & Lacey Police Department (LPD)

Purpose

NTPS will provide limited, view-only access to the Skyward Student Information System (SIS) and access to the district video management system (VMS) for LPD School Resource Officers (SROs) and designated SRO Supervisors to support school safety and student-support functions.

Authority & Compliance

This Agreement is executed under the authority of the Interlocal Cooperation Act and satisfies the requirements of RCW 39.34.240, which mandates a written data-sharing agreement when a public agency requests access to Category 3 or higher confidential information. Such agreements must conform to the policies of the Washington State Office of Cybersecurity.

This Agreement conforms to statewide cybersecurity requirements, including WaTech SEC-08 Data Sharing Policy, which establishes required components for sharing protected data—purpose, authority, classification, permitted uses, authorized users, security safeguards, retention and disposal, incident-response processes, and training.

All access to and use of SIS data and FERPA-protected VMS footage will comply with FERPA, including NTPS's obligation to maintain direct control over education records, limit redisclosure, and document emergency disclosures as required under 34 CFR § 99.32(a)(5).

Data Covered

Access includes: Family/guardian contact information, attendance data, and discipline records.

For the VMS, this agreement applies only to video that qualifies as a FERPA-protected education record, meaning video that is directly related to a student and maintained by NTPS. Examples include video depicting student misconduct, injury, victimization, violations of law or policy, or situations where a student is the specific focus of the recording.

Video that is not directly related to a student (e.g., adult-only incidents, property crimes, incidental student background presence) is *not* an education record and is outside the scope of this Agreement. Such non-FERPA video may be disclosed to law enforcement under state law.

Excluded unless separately authorized: IEP/504 records, student health or medical records, counseling records, and any SIS/VMS data not expressly included above.

Off-hours access: SIS directory-level access (student name, birth date, guardian contacts) may be provided to one designated LPD supervisor per shift for emergency response purposes.

Authorized Users

Access is limited to SROs and SRO Supervisors designated by LPD. Access to contact information is limited to supervisors designated for off-hours access. LPD will maintain a current roster and notify NTPS of staffing changes within two business days.

Permitted Uses

Access may only be used to support school safety and security, coordinate with administrators on school-based incidents, contact families for urgent safety reasons, or respond to a health/safety emergency under 34 CFR § 99.36.

Emergency Information Access (Exigent Circumstances)

In exigent circumstances involving an immediate and significant threat to the health or safety of students, staff, or the public, NTPS may disclose or provide temporary access to FERPA-protected SIS data and FERPA-protected VMS footage to LPD under FERPA's health or safety emergency exception (34 CFR § 99.36).

Only the minimum necessary information will be disclosed. NTPS will document these disclosures as required by 34 CFR § 99.32(a)(5).

Video that does not directly relate to a student is outside the scope of this Agreement and may be disclosed separately under state law.

Threat Assessment Team (TAT) Access (Non-Emergency, Case-Specific)

When participating as part of the NTPS Threat Assessment Team (TAT), LPD SROs and SRO Supervisors may receive case-specific student information not otherwise included in this Agreement when necessary to perform their assigned TAT responsibilities.

These disclosures occur under FERPA's "school official with legitimate educational interest" exception (34 CFR § 99.31(a)(1)(i)), which allows disclosures to outside parties who perform institutional functions NTPS would otherwise use its own employees to perform, who are under NTPS's direct control regarding the use and maintenance of the records, and who are subject to FERPA's redisclosure limitations.

Permissible TAT-related disclosures may include records directly relevant to the threat assessment process (e.g., attendance patterns, disciplinary history, academic engagement concerns, situational safety information). Access must be limited to the minimum information necessary, and only for the duration of the TAT process.

This clause applies only to non-emergency threat assessment activities. Emergency disclosures remain governed by the Exigent Circumstances clause above.

Prohibited Uses

LPD will not use SIS or VMS access for unrelated investigations. Redisclosure is prohibited unless allowed by FERPA. LPD will not create copies of SIS or VMS data unless NTPS provides or authorizes the copy.

Use of Copies

LPD may store and use any SIS or VMS records that NTPS provides to LPD, including placing such records into LPD's evidence systems as required by law-enforcement procedures. When only viewing information inside NTPS systems, LPD will not download or create a copy unless NTPS provides or authorizes one.

Security Requirements

Individual, non-shared accounts; least-privilege access; MFA/SSO where supported; encrypted devices; screen lock; no screenshots or downloads unless authorized. NTPS may suspend access immediately if needed.

Incident Reporting

LPD must notify NTPS within 24/48 hours of any suspected or confirmed unauthorized access or disclosure and cooperate in investigation and mitigation.

Retention & Disposal

If NTPS authorizes a specific export, LPD will retain the data only as long as necessary for the authorized purpose and will destroy it in accordance with LPD's established evidence-retention and destruction procedures. Upon request, LPD will confirm that destruction was completed consistent with those procedures.

Public Records

Each Party will independently fulfill its obligations under the Washington Public Records Act (RCW 42.56). This Agreement does not require either Party to notify the other when a public records request is received. Each Party will apply all legally required redactions, including those protecting FERPA covered student information.

Training

LPD will ensure that all SROs, Supervisors, and off-hours supervisors with access to district data complete annual FERPA and data-security training, consistent with statewide cybersecurity requirements.

Signatures

NTPS: _____ Date: 3/27/26

LPD: _____ Date: 3/27/2026

