G-0331 **GBC-E**

Criminal History Record Information Acceptable Use and User Acknowledgment

Purpose

Aztec Municipal Schools permits access to Criminal History Record Information only when access is required for an authorized District duty. This agreement states the rules each user must follow before access is granted and while access continues.

Conditions of Access

- My access must be approved in advance and limited to the least privilege necessary for my assigned duties.
- I must complete required security-awareness and role-based training before access and at least annually thereafter.
- I must sign this agreement before access, re-acknowledge it annually, and sign the current version when it is revised or my responsibilities change.
- My access is a limited work privilege and may be logged, monitored, audited, suspended, or revoked.

Authorized Use

I may access or use CHRI only when all of the following are true:

- The use is part of my assigned District duties and is authorized by law, District policy, NMDPS and FBI requirements, and the District's applicable account authority.
- The CHRI concerns the specific applicant, employee, volunteer, contractor, or contractor employee whose assigned decision I am handling.
- The use is limited to the original authorized purpose. I will request a current record through the approved process if a later or different authorized use requires one.
- I view or discuss only the minimum necessary information and only with authorized recipients directly involved in the specific decision.
- I follow all required notice, identity-verification, accuracy, review, challenge, correction, and adverse-decision procedures.

Prohibited Use and Disclosure

I will not:

- Access CHRI out of curiosity or for a personal, political, retaliatory, discriminatory, commercial, or other unauthorized purpose, including checking myself, relatives, friends, coworkers, public figures, or anyone outside an assigned case.
- Confirm or deny that CHRI exists to anyone who is not authorized to receive it.
- Discuss, display, forward, copy, photograph, screenshot, print, download, upload, or otherwise reproduce CHRI except as specifically required by an approved workflow.
- Disclose CHRI to another department, school, agency, vendor, attorney, insurer, reference checker, records requester, applicant, or other person unless the disclosure is specifically authorized and handled through the District's approved process.

- Enter CHRI into a public or consumer artificial-intelligence system, external chatbot, personal email, personal cloud storage, social media, unapproved application, or unapproved website.
- Use a personal device, removable media, public computer, or unapproved network, account, application, or location to access, store, process, or transmit CHRI.
- Share a password, authentication code, account, badge, key, or authentication device; permit another person to work under my identity; or bypass security controls or logging.
- Treat an arrest alone as proof of misconduct or make a suitability decision outside approved District procedures and applicable law.

Account Workstation and Paper Security

- I will use only the unique account assigned to me and required multifactor authentication.
- I will verify the subject and authorized purpose before opening a record and verify the recipient before any permitted communication.
- I will lock the screen or sign out whenever I leave the workstation and position screens and documents to prevent unauthorized viewing.
- I will not leave CHRI unattended at a printer, scanner, copier, desk, meeting room, vehicle, or other uncontrolled location.
- I will keep any authorized temporary paper copy under my direct control or in the approved locked location and return it for approved destruction immediately after use.

Records Requests and Legal Demands

I will route any subpoena, discovery request, public-records request, law-enforcement request, or other demand for CHRI immediately to the Superintendent or designee, records custodian, and District legal counsel. I will not release CHRI independently.

Security Incident Reporting

I will immediately report, and in every case report no later than one hour after discovery, any lost or misdirected record, unauthorized viewing or disclosure, suspicious access, mistaken email or printout, lost device or credential, malware, phishing, system anomaly, policy violation, or other concern that CHRI may have been exposed. I will report to the Authorized Recipient Security Officer and Point of Contact using the current District contact instructions.

- I will preserve evidence, record what occurred and when, and follow response instructions.
- I will not conceal the event, alter or delete evidence, contact an affected person, or conduct my own investigation unless directed.
- I understand that prompt good-faith reporting is required even if I caused the error or am unsure whether an incident occurred.

Transfer Separation and Continuing Confidentiality

I will promptly notify the Point of Contact or Authorized Recipient Security Officer if my duties no longer require access or my access appears broader than necessary. The District may change or disable access and retrieve credentials, equipment, media, and materials when my assignment, status, or duties change. My duty to protect CHRI continues after my access and employment or service end.

Monitoring Audits and Consequences

The District and authorized oversight entities may log, monitor, review, inspect, and audit CHRI access and related systems, records, and procedures. I will cooperate with authorized audits and investigations and will not alter or destroy relevant evidence.

Failure to comply may result in immediate suspension or revocation of access, retraining, corrective or disciplinary action up to and including discharge or termination, contract action, referral to licensing or oversight authorities, civil liability, or criminal prosecution. Any employment action will be taken in accordance with applicable law, the collective bargaining agreement, contracts, and District policy.

User Certification

By signing below, I certify that I have received, read, and understand GBC, GBC-R, and this agreement. I agree to follow them and all applicable District, NMDPS, FBI, state, and federal requirements. I understand the limits on my access, my duty to report suspected incidents, the consequences of misuse, and my continuing confidentiality obligation.

Printed name	
Position and department	
Signature	
Date	
Training completion date	
Access approved by	
Approval date	

District Reporting Contacts

The Authorized Recipient Security Officer is the Deputy Superintendent unless another qualified employee is designated in writing. The Point of Contact is the Employee Services Specialist unless another qualified employee is designated in writing. Current telephone, email, after-hours, and alternate reporting instructions shall be provided to every authorized user and maintained with this acknowledgment.