DECAL Compliance Guide for Identity Verification of GAPREK Users

Through the Online Access Agreement for the Georgia Department of Early Care and Learning (DECAL) Georgia's Pre-K Online System (GAPREK), the Primary Authorized User is responsible for complying with applicable laws, regulations, standards, and best practices when creating user IDs and passwords for their organization. This document is a guide to compliance with such requirements and **is meant to be an overview, not a substitute for careful review of applicable laws, regulations, and guidance.**

By signing the Online Access Agreement, the Primary Authorized User agrees to verify users' identities in accordance with NIST 800-63A requirements for Identity Assurance Level 2; protect personally identifiable information (PII) to ensure confidentiality, integrity, and availability; and protect the security of user IDs and password combinations.

Because the GAPREK system contains confidential data, users who access the system are required to prove their identity (similar to entering personal information to prove your identity when registering for online banking or a health provider portal). As stated in the NIST 800-63A guidance, the "enrollment and identity proofing process should be designed and implemented so it is easy for users to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens."

Identity Proofing
Identity proofing is the process by which a Credential Service Provider (in this case, the Primary Authorized User for GAPREK) collects and verifies information about an individual for the purpose of issuing credentials to that individual. Identity is proven by verification of identification evidence (documentation submitted to prove an individual's identity).

General guidelines for identity proofing include:

- Collection of PII must be limited to the minimum necessary to validate an identity.
- Notice must be provided at the time of, or prior to, evidence collection to the individual whose identity is being proven. The notice should include, but is not limited to:
    a. The types of personal information necessary for collection purposes;
    b. Whether such information is mandatory or voluntary;
    c. Purposes for the collection and maintenance of personal information and attributes;
    d. Whether the information will be retained and how it will be protected; and
    e. Consequences for failure to provide required information.
- Attributes (e.g., name, date of birth) should only be used for identity proofing or to comply with a law or legal process unless notice is given to or consent provided by the individual.
- There must be a process through which individuals can report complaints or problems arising from identity proofing that is easy to find and use.
- The process for identity proofing should be documented in a written policy or practice statement that specifies the steps used for identity proofing and enrollment.

This policy or statement should also detail procedures for addressing errors and circumstances that result in failure to successfully enroll applicants in the identity system (e.g., if a person does not become employed at the organization or fails to provide the required identity evidence).

- A record must be maintained, including audit logs, of all steps taken to verify an identity and the types of identity evidence presented in the proofing process.
    a. A risk management process must be conducted to determine:
        i. Any steps that it will take to verify the individual's identity beyond any mandatory requirements;
        ii. The PII, including any biometrics, images, scans, or other copies of the identity evidence, that will be maintained as a record of identity proofing; and
        iii. The schedule of retention for these records in accordance with applicable laws, regulations, and policies.
- All PII collected must be protected to ensure confidentiality, integrity, and attribution of the information source.
- Identity proofing may occur in person or remotely. If remote verification is completed, reach out to DECAL for additional information.
- Sensitive data, including PII, must be disposed of or destroyed if identity proofing processes are no longer conducted.
- Social Security Numbers should not be collected unless it is necessary for identity proofing and identity proofing cannot be accomplished by collection of another attribute or combination of attributes.
- Address of record must be confirmed, ideally through validation of the address contained on any supplied identity evidence. Self-asserted address data must not be used for confirmation.
    a. Valid records to confirm address must be the issuing or authoritative source(s).

The identity proofing process is made up of three steps: resolution, validation, and verification. Each step is outlined below. For more in-depth information and guidance, please review the NIST 800-63A standard.

1. Resolution

The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the minimum set of attributes necessary to distinguish an individual. Such attributes may include but are not limited to: name, address, date of birth, email address, and phone number.

Acceptable identity evidence, listed in the table below, can be traced to issuing sources, such as state motor vehicle departments, state/federal government agencies, law enforcement agencies, utility companies, and/or financial institutions.

Superior Identity Evidence (not a comprehensive list)	**Strong+ Identity Evidence*** (not a comprehensive list)
U.S. Passport or U.S. Passport Card	State-issued REAL ID card
Foreign e-passport	State-issued Enhanced ID card
Person Identity Verification (PIV) card	U.S. Military ID
Permanent Resident Card issued on or after May 11, 2010	
Native American Enhanced Tribal card	

*Evidence above listed as "Strong+" must be validated with the respective State Department of Motor Vehicles, DMV databases maintained by the American Association of Motor Vehicle Administrators (AAMVA), or military-issuing source.

If there are conflicts among attribute information (e.g., name or address), knowledge-based verification may be used but only for one piece of validated identity evidence. Knowledge-based verification occurs when an identity is verified based on knowledge of private information associated with the claimed identity. An example of knowledge-based verification includes asking security questions that only the individual would know. The individual whose identity is being resolved must be allowed to opt out of knowledge-based verification. Information accessible freely, for a fee in the public domain, or obtained illegally must not be used for knowledge-based verification.

2. Validation

The goal of identity validation is to determine the authenticity, validity, and accuracy of the collected identity evidence. The process of identity validation contains two steps:

1. Confirm the evidence is genuine and authentic;
2. Confirm the data contained on the identity evidence is valid, current, and related to an actual, live individual.

Validating the evidence involves examining the evidence for:

- Confirmation of required information completeness and format for the identity evidence type;
- Detection of evidence tampering or the creation of counterfeit or fraudulent evidence;
- Confirmation of security features (e.g., holographic images)

Acceptable identity evidence (listed above) must be confirmed as genuine by trained personnel or appropriate technologies.

When possible, all personal and evidence details should be confirmed as valid by comparison with information held or published by the issuing or authoritative source(s). The results of identity evidence information validation and evidence genuineness validation should be recorded in enrollment records or audit logs.

3. Verification

Identity verification represents the processes of confirming that the evidence, previously shown to be valid, actually refers to the individual that is appearing for identity proofing. This is done by a physical or biometric comparison between information on the identity evidence and a biometric characteristic obtained from the individual.

The identity evidence may be verified through biometric verification. For example, the facial image on a passport or driver's license can be compared to the individual's facial image in person.

If remote verification is required, reach out to DECAL for additional information.