

Student PII and FAA Remote Pilot Certification

Privacy and Operational Guidance for High School Drone Programs

Prepared for: School districts, CTE leaders, privacy officers, administrators, instructors, students, and families

Prepared by: Blue Ridge Mountain Drones Education and DronePilotsForUS
September 2026

Central conclusion

Schools can support students through FAA Remote Pilot certification without becoming repositories for unnecessary personal data. The safest model uses student- or parent-controlled accounts, truthful FAA submissions entered directly by the applicant, minimal school retention, clear family notice, and district review of applicable state and local requirements.

This paper provides program and policy guidance, not legal advice. District counsel or the privacy officer should review the final local procedure.

Executive Summary

FAA certification activities require accurate identity and contact information, but they do not require a school to collect or retain every data element submitted by a student. FERPA applies to personally identifiable information in education records maintained by a school or a party acting for it. Whether a particular FAA-registration activity implicates FERPA therefore depends on how the school structures, requires, observes, transmits, and records the activity—not simply on whose fingers type the information.

A defensible high-school implementation separates instruction from identity processing. The school teaches aviation knowledge and explains the certification pathway; the student and parent control the account and enter sensitive information directly into FAA or authorized testing systems. Staff verify only the minimum evidence needed for legitimate program purposes and follow district retention rules.

Key Findings

Issue	What current federal materials establish	Recommended district practice
Eligibility and age	A person may take the Unmanned Aircraft General knowledge test at age 14; a Remote Pilot Certificate requires age 16 and the other eligibility criteria in 14 CFR §107.61.	Do not describe a passing test by a 14- or 15-year-old as an issued certificate. Plan the timing of IACRA application accordingly.
FAA data	IACRA uses an FAA Tracking Number and collects personal details. A valid email and residential address are part of the application process; SSN disclosure is optional.	Use a student-controlled, durable email. Have the applicant enter accurate data directly; never invent or substitute identity information.
FERPA	FERPA protects PII in education records maintained by the school or a party acting for it and limits nonconsensual disclosure unless an exception applies.	Do not assume direct student typing ends the analysis. Map the data flow, vendor role, school records, purpose, consent/exception, and state law.
Public registry	FAA does not display SSN, certificate number, or date of birth in Airmen Inquiry. A releasable address may appear unless the airman elects not to release it.	Tell families about address releasability and show certificated students how to manage it through FAA Airmen Services.

1. Scope and Definitions

Student PII is a broad operational term. Under FERPA, personally identifiable information includes direct identifiers, indirect identifiers, and combinations of information that would allow a reasonable person in the school community to identify a student. FERPA's disclosure restrictions attach when that information is contained in an education record maintained by the school or by a party acting for it.

- Examples relevant to certification include legal name, date of birth, residential and mailing addresses, email, government-ID details, FAA Tracking Number (FTN), test information, and certificate status.
- Not every item handled by a student is automatically a school education record; conversely, data can become part of a school record if the district captures or maintains it.
- State student-data privacy laws, district policy, contracts, record schedules, and cybersecurity rules may impose duties beyond FERPA.

2. FAA Remote Pilot Certification Pathway

Stage	Applicant action	School boundary
Create IACRA profile	Register personally, obtain an FTN, use accurate identity and contact information.	Teach the process; do not create a shared account or retain the password.
Schedule and test	Use the FTN; present acceptable identification; take the UAG knowledge test.	A school may support preparation and logistics without copying the applicant's full ID.
Apply for certificate	After passing and once eligible, complete FAA Form 8710-13 in IACRA, review the Privacy Act statement, and submit.	Avoid proxy completion. Staff may provide navigation help while the applicant controls the screen and attests to accuracy.
Maintain record	Keep FAA contact information current and manage address releasability.	Retain only the proof the district has a documented need and authority to maintain.

The FAA's Unmanned Aircraft Systems Airman Certification Standards states that an applicant must be at least 14 to take the knowledge test and at least 16 to hold the certificate. Test-center identity requirements include an acceptable government-issued photo ID with signature and date of birth. When a mailing address is a post office box, the applicant must also provide a residential address.

3. What IACRA Collects—and What Schools Need Not Collect

IACRA's privacy statement ties the collection to federal aviation certification authorities and DOT/FAA 847, Aviation Records on Individuals. FAA materials state that a valid email is needed for registration and that additional information, including residential address, is required when the applicant starts an application. The Social Security number is optional.

Data element	FAA/testing use	Recommended school handling
Legal name and date of birth	Identity matching, testing, eligibility, and security vetting.	Applicant enters directly. Do not store a separate class roster containing DOB unless the district has a defined need and protection plan.
Residential/mailling address	Application, certificate delivery, and airman record. Residence may be required even if a PO box is used for mail.	Do not substitute a school address for the student's true residence. Avoid viewing or retaining it unless necessary and authorized.
Email	Account access, FTN communications, recovery, and notices.	Recommend a durable personal email controlled by the student/family. A school email is not categorically forbidden, but it may expire or be monitored.
SSN	Optional identifier in IACRA.	Do not request, record, or direct a student to disclose it for this activity.
Government ID	Test-center identity verification.	Explain acceptable ID in advance. Do not photocopy or photograph it absent a separately approved need.
FTN/test/certificate status	Links the applicant to knowledge testing and certification.	Treat as sensitive program information. Record the minimum status evidence required, not account credentials or complete FAA screens.

4. FERPA: Avoid the 'Direct Entry' Shortcut

The statement that student-entered data is always outside FERPA is too broad. Department of Education guidance defines education records by relationship to the student and maintenance by the

school or a party acting for it. When a district requires a third-party service for a school activity, prepopulates the service, receives results, records identifiers, or contracts with the provider, FERPA and district obligations may be implicated.

A student acting independently in a personal capacity is different from a school-directed workflow. The practical question is the full data lifecycle: Who requires the activity? Who supplies the data? Who can see it? Where is it transmitted? What does the school or vendor retain? What record is returned? What legal authority supports each disclosure?

Federal analysis questions

- Is the information directly related to a student and maintained by the school or a party acting for it?
- Does the school disclose education-record PII to FAA, a testing vendor, or another party? If so, is there consent or a documented FERPA exception?
- Is a vendor performing an institutional service under the school's direct control with appropriate limits on use and redisclosure?
- Does the district maintain test outcomes, FTNs, copies of IDs, or certificate records, and for how long?
- Do state law, board policy, or parent-notice requirements impose additional protections?

5. Recommended Privacy-by-Design Model

Role	Primary responsibilities
Student and parent/guardian	Control the email and IACRA credentials; enter and verify identity/contact data; bring acceptable ID; manage FAA address and releasability choices.
Instructor	Teach the pathway; provide neutral navigation support; avoid collecting passwords, SSNs, ID scans, DOB/address lists, or screenshots containing PII.
CTE/program administrator	Define the legitimate educational record, minimum proof, access roles, retention period, and approved communication method.
District privacy/legal staff	Review FERPA, state law, vendor terms, parent/student notice, accessibility, cybersecurity, and records management before launch.
Testing coordinator/provider	Communicate official eligibility and ID rules; protect testing records; use approved data-transfer channels.

Minimum-data rules

- No shared IACRA accounts, shared passwords, or teacher-controlled student accounts.
- No class spreadsheet containing full DOB, residential address, FTN, ID number, and test result unless specifically approved and secured.
- No screenshots of account pages or IDs as routine evidence.
- Use a status-only record when possible, such as 'knowledge test passed—date verified' or 'certificate viewed—date verified.'
- Limit access to personnel with a documented educational need; delete or archive according to the approved retention schedule.

6. Standard Operating Procedure

When	Required action	Control
Before instruction	District privacy/legal review; approve the data-flow map, notices, vendor/testing arrangements, and retention schedule.	Document the owner and approval date.
Before registration	Provide student/family notice explaining FAA data, age rules, identity requirements, public-record choices, and school records.	Use acknowledgement or consent only as required by applicable law/policy; do not mislabel a notice as legal consent.
During registration	Student/parent creates the account and enters data on a private screen.	Instructor may explain fields but should not request credentials or transcribe sensitive values.
Before testing	Confirm official eligibility, FTN, and acceptable-ID requirements using current FAA/PSI instructions.	Do not copy the ID merely to prove readiness.
After testing	Student receives results and completes IACRA application when eligible.	School records only the minimum approved status evidence.
After certification	Student updates FAA address within required timeframes and chooses address releasability.	Provide the FAA Airmen Services link; do not promise that all airman information is private.

7. Parent and Student Notice: Required Content

A local notice should be plain-language, accessible, and provided before account creation or testing. It should identify:

- the educational purpose and whether certification is required or optional;
- the FAA and testing systems the student will use, with links to their current privacy statements;
- the data the student will submit and which data the school will—not merely may—retain;
- the difference between age 14 test eligibility and age 16 certificate eligibility;
- the possibility of public release of a releasable airman address and how to change that preference;
- the district contact for privacy, records, accessibility, and alternative arrangements; and
- the applicable retention period and complaint/correction process.

Districts should not imply that a family waives statutory rights by signing an acknowledgement. Counsel should determine whether consent is needed for any school disclosure and whether an available FERPA exception is appropriate.

8. Risk Scenarios and Controls

Scenario	Risk	Preferred control
Teacher collects student DOB and home address in a class spreadsheet	Creates a concentrated school record with identity-theft and unauthorized-disclosure risk.	Student enters data directly in FAA/testing systems; school keeps only approved status evidence.
Registration screen is projected or shared	Peers may see identity, address, FTN, or account data.	Use individual/private screens and privacy filters where appropriate.
All students use one school email or password	Account attribution, security, recovery, and applicant control fail.	One applicant-controlled account per person; never share credentials.

Scenario	Risk	Preferred control
School email expires after graduation	Student may lose recovery and notice access.	Recommend a durable personal email and maintain recovery information privately.
School scans IDs 'just in case'	Unnecessary collection expands breach and retention exposure.	Explain official ID rules; let the testing provider inspect the original.
Teacher substitutes school address for residence	FAA record may be inaccurate; mail and identification may not match.	Use truthful residence data. If a PO box is used for mail, also provide residence as required.
Certificate status is posted publicly	Unnecessary disclosure of a student's accomplishment and associated identity.	Use internal access controls and obtain appropriate authorization for publicity.

9. Model District Policy Position

The district supports students pursuing FAA Remote Pilot certification while minimizing institutional collection of personal data. Students and parents control individual FAA and testing accounts and submit accurate information directly to authorized systems. Employees do not collect passwords, optional Social Security numbers, routine copies of government identification, or unnecessary residential and birth information. The district documents any education records it maintains, the legal basis for disclosures, authorized access, safeguards, retention, and deletion. Certification support is implemented only after review under FERPA, applicable state law, board policy, cybersecurity standards, and current FAA/testing requirements.

10. Implementation Checklist

Check	Program evidence
☐ Current official requirements verified	Date checked; FAA/PSI pages used; staff owner.
☐ Data-flow map approved	Fields, systems, users, transmissions, school records, and retention identified.
☐ Family notice approved	Purpose, data, age, public registry, school retention, contacts, and alternatives included.
☐ Accounts remain applicant-controlled	No shared credentials; durable email guidance provided.
☐ Private registration workflow	No projected screens, routine screenshots, or staff transcription of PII.
☐ Minimum evidence defined	Approved status-only record and retention period documented.
☐ Incident process ready	District reporting, containment, family communication, and vendor escalation documented.

11. Legal and Regulatory Sources

- [FAA — IACRA Privacy Act Statement](#) — Authority, information collection, optional SSN, DOT/FAA 847, and public-record notice.
- [FAA — IACRA Registration Help](#) — Valid email, FTN registration, and residential-address information.
- [FAA — Remote Pilot Application Guide](#) — Application workflow, identity information, test ID, Privacy Act review, and temporary certificate.

- [FAA — UAS Airman Certification Standards](#) — Age thresholds, FTN, and knowledge-test identification/address requirements.
- [FAA — Advisory Circular 61-65H](#) — Identification, age, mailing, and residence-address guidance.
- [FAA — Airmen Inquiry](#) — Fields excluded from public display and address-releasability notice.
- [FAA — Airmen Services](#) — Address updates and address-releasability services.
- [FAA — Change of Address](#) — Thirty-day update requirement and residence/PO-box distinction.
- [DOT — Airmen Certification System PIA](#) — Current privacy-impact overview for the airmen certification system.
- [DOT — Privacy Act System of Records Notices](#) — DOT/FAA 847, Aviation Records on Individuals.
- [U.S. Department of Education — What is an education record?](#) — FERPA definition of an education record.
- [U.S. Department of Education — PII from education records](#) — FERPA definition and examples of PII.
- [U.S. Department of Education — Disclosure](#) — FERPA disclosure concepts.
- [U.S. Department of Education — Online Educational Services Guidance](#) — FERPA analysis and best practices for school use of third-party online services.
- [U.S. Department of Education — Data Security](#) — K–12 privacy and security resources.

Conclusion

A school does not need to choose between student opportunity and student privacy. It can deliver rigorous Part 107 preparation while keeping applicant identity processing where it belongs: in applicant-controlled interactions with authorized FAA and testing systems. The governing principle is data minimization supported by accurate notice, documented authority, secure handling, and current-source verification.

Because FAA processes, vendor practices, and state student-privacy laws can change, districts should revalidate the workflow before each program year.