

# Online Proctoring: Selection & Privacy Checklist

A one-page gate to run before you proctor: pick the lightest defensible approach, clear the consent and biometric-law questions, and set retention. Engineering guidance, not legal advice.

---

## A. Choose the lightest defensible approach

---

- Confirm the exam is high-stakes enough to justify proctoring at all
- Considered cheat-resistant assessment design as the primary control first
- Matched the approach to need: live (intervene), record-and-review, or automated
- Budgeted human review of automated flags (est. 5-8% false positives)

## B. Consent & biometric law

---

- Written, informed consent obtained before any faceprint is collected (BIPA)
- Lawful basis + GDPR Art 9 condition documented for EU/UK test-takers
- No emotion / stress inference (banned in EU education since Feb 2025)
- Avoided routine room scans; reviewed Ogletree (4th Amendment) for public bodies

## C. Fairness & accessibility

---

- Face detection tested across skin tones, lighting, and camera quality
- Accommodations for disabled, neurodivergent, and caregiving test-takers
- Every flag reviewed by a human with context; no automatic fail
- Documented appeal route for a wrongly flagged test-taker

## D. Data, retention & security

---

- Data-processing agreement (GDPR Art 28) signed with the proctoring vendor
- Collect the least data needed; retention period defined and enforced
- Recordings and biometric data encrypted in transit and at rest
- EU AI Act high-risk duties checked for automated proctoring (from Aug 2026)