

YearbookLife

Student Photo Privacy Checklist

Protecting student images requires strong contracts, secure systems, and clear internal controls. Use this checklist to evaluate your school's current student photo privacy practices.

1. Photographer Contract Review

- Copyright ownership clearly defined
- School usage rights documented in writing
- AI training and facial recognition explicitly prohibited
- Student images may not be sold or shared with third parties
- Data retention timelines specified
- Photographer provides written privacy policy

2. Vendor & Yearbook Platform Safeguards

- Secure storage systems in place
- Permission-based access (role-restricted logins)
- No AI training or data mining of student images
- Images used solely for school publishing purposes
- Vendor complies with FERPA and applicable state laws

3. Internal Access Controls

- Access limited to authorized staff and supervised students
- Secure passwords required
- Access revoked at end of school year
- No storing images on personal devices
- Downloading and sharing monitored

4. Parent Transparency

- Written student image policy exists
- Parents informed how photos are used
- Opt-out procedures documented (where applicable)

- Clear process for image concerns or removal requests

5. Data Storage & Retention

- Images stored in secure systems
 - Retention timelines defined
 - Archived images reviewed periodically
 - Deletion procedures documented
-

Complimentary Resource: Download the full Student Image Protection Policy Template at www.yearbooklife.com © 2026 YearbookLife | Independently Operated | Yearbook Publishing & Software