ASSETBANK

Content compliance & control in higher education

Managing consent, usage & digital assets across universities

Why this matters

Universities create and manage vast volumes of content, from student photography and video to campaign assets and research communications.

But with increasing scrutiny around GDPR, consent, and usage rights, managing digital assets is no longer just an operational challenge - it's a compliance priority.

The challenge

- Content spread across regions, departments, and teams
- Consent forms stored separately from assets
- Inconsistent usage across channels and campaigns
- Limited visibility over what's safe to use

The result?

Increased risk, inefficiency and lack of control

Missing consent forms

Where universities are exposed

Using student or staff imagery without valid or current consent

Reusing assets beyond agreed usage terms

Losing track of expiry dates for permissions

Lack of clarity over who can access and use assets

What “good” looks like

A compliant, scalable approach to content

1. Centralised asset management

all content stored in one place with clear governance.

2. Linked consent & rights

consent, licences, and permissions tied directly to each asset.

3. Controlled access

teams only access assets they are approved to use.

4. Full visibility

clear indicators of usage rights and compliance status.

Consent & usage audit checklist for university marketing teams

Stay compliant. Stay in control.

Before you start

Use this checklist to audit your digital assets including images, video, and campaign content – to ensure they are compliant, approved, and safe to use.

1. Consent & release forms

- [ ] Do all images and videos featuring identifiable individuals have valid consent?
- [ ] Are consent forms stored and linked to each asset?
- [ ] Can you quickly find all assets linked to a specific individual?
- [ ] Do you have a process for handling withdrawn consent?
- [ ] Are parental/guardian consents tracked where required?

Best practice

Link consent directly to assets and keep it visible and auditable.

2. Usage rights & licensing

- [ ] Is ownership or licensing clearly defined for every asset?
- [ ] Are usage restrictions (e.g., editorial only, web only) clearly visible?
- [ ] Are photographer credits consistently applied?
- [ ] Are licence terms embedded or attached to the asset?
- [ ] Are users reminded of rights before download?

Please note

Without clear rights visibility, teams risk misuse and compliance breaches.

3. Expiry dates & permissions

- [ ] Do assets have expiry dates for consent and licences?
- [ ] Are expired assets automatically hidden or restricted?
- [ ] Are alerts in place before consent or licences expire?
- [ ] Are outdated assets archived or removed from use?

Remember

Consent and licences expiring without notice is a major GDPR risk.

4. Access & permissions control

- [ ] Can you control who sees and downloads specific assets?
- [ ] Are permissions set by department, role, or region?
- [ ] Are sensitive assets restricted or approval-based?
- [ ] Do external partners only access approved content?

Please note

Granular permissions ensure the right people access the right assets and nothing more.

5. Audit trail & accountability

- [ ] Can you track who has downloaded or used assets?
- [ ] Do you have a clear audit trail for compliance checks?
- [ ] Are approvals required for sensitive asset use?
- [ ] Can you generate reports to prove compliance?

Remember

Audit-ready records are essential for regulatory and internal governance.

6. Metadata & organisation

- [ ] Does every asset include structured metadata (consent, rights, expiry)?
- [ ] Can users filter assets by usage permissions?
- [ ] Are naming conventions consistent across teams?
- [ ] Can you quickly find compliant, approved assets only?

Please note

Metadata is the backbone of compliant asset management.

7. Video & AI content compliance

- [ ] Do videos have consent for all identifiable individuals (including audio)?
- [ ] Are filming locations and usage rights documented?
- [ ] Is AI-generated content clearly labelled and governed?
- [ ] Do you understand ownership and usage rights for AI assets?
- [ ] Are video assets reviewed for compliance before publishing?

Remember

Audit-ready records are essential for regulatory and internal governance.

Red flags to watch for

- Assets stored across shared drives and folders
- Missing or unclear consent documentation
- Expired licences still in use
- Teams unsure what they can/can't use
- No audit trail or reporting

Final check

If you answered “no” or “not sure” to any of the above, your university may be exposed to:

GDPR and privacy risks

Copyright and licensing breaches

Reputational damage

Inefficient workflows and duplicated work

Ask yourself:

Do we have consent for every identifiable person in this content?

Do we know where that consent lives?

Are we using assets within their agreed purpose?

Do we understand the rights attached to AI-generated content?

How Asset Bank helps

- Centralised asset storage with built-in consent and rights management
- Clear, visible usage rights at every stage
- Automatically initiate compliance actions - not just expiry reminders
- Granular permissions across teams and departments
- Full audit trails and reporting

Use assets confidently. Control access. Protect rights.

We're trusted by global universities

The Open University

Goldsmiths
UNIVERSITY OF LONDON

University of BRISTOL

UNIVERSITY OF BIRMINGHAM

Explore how we can help you

Book a demo to see how Asset Bank helps universities stay compliant.

We offer a 10% discount to all higher education clients

Book a demo today