



## Blackboard Collaborate – Built to support data protection

Blackboard Collaborate is a virtual classroom solution that supports your data protection obligations. If you're looking for a solution that won't share user data with advertisers and social media companies, then look no further than Blackboard Collaborate.

Blackboard cares about data protection. We know that our clients' data is entrusted to us and take our data protection obligations very seriously. We therefore apply the standards of the EU General Data Protection Regulation (GDPR) globally. Our products are designed to meet the requirements of data protection regulations around the world including the GDPR, the South African Protection of Personal Information Act (POPIA) and the Australian Privacy Act, to name just a few.

The information below gives you a quick overview of our approach to helping you meet your data protection responsibilities and lists some helpful privacy and security best practices\*.

### Data protection compliance with Blackboard Collaborate

- Blackboard Collaborate is designed for education and to help universities, schools and organisations with their data protection obligations
- You own your data; we just look after it for you
- No ifs or buts: We don't use or share user data for marketing or advertising purposes
- We don't share your data with social media companies
- We don't have user tracking functionalities that can cause student rebellions, like checking if users focus on their screens
- We only use user data as instructed by our clients
- Our data processing agreement (DPA) meets the requirements of the EU General Data Protection Regulation (GDPR)
- Users are notified when sessions and chats are recorded
- You can anonymise chat contributions
- We responsibly delete client data 30-days after the contract term ends
- We offer secure user authentication through Blackboard Learn
- Data is encrypted when traversing the open internet
- We build on Amazon Web Services' industry-leading hosting security controls
- Regional hosting (e.g. EU clients hosted in AWS EU data centres)

# Privacy and security best practices

## Administrators

- [Integrate with Blackboard Learn](#) to securely authenticate your users and to avoid unauthorised users gate crashing your sessions

## Instructors (“Moderators”)

- Review your session material and remove identifying information unless it is required
- Remember to switch off notifications and close other applications before sharing your screen
- Blackboard Collaborate notifies users when sessions are recorded, but it’s still good practice to also announce it
- You can [anonymize chat recordings](#)
- Restrict [attendee moderator/presenter](#) rights to those who need it when you set up your Collaborate session
- Share guest links mindfully as they are public links. Use the Invite attendee feature to create secure links that can’t be shared.
- Additional best practices can be found on our [Help pages](#)

## Users (“Participants”)

- Think before you share information about yourself and others in sessions. Particularly when sessions are recorded.
- Mute yourself when not speaking
- You can chat [privately with others](#) (but remember that the moderators may still supervise those chats)
- Follow your institution’s guidelines on the acceptable use of IT tools
- Additional best practices can be found on our [Help pages](#)

If you have any feedback or would like us to include anything else, please post your feedback it in our [Data Privacy and Security Community group](#).

\* The above information is for guidance only and does not constitute legal or professional advice. Please make sure you consult with your legal/privacy team.