



Digital Delivery of Unloc Services Safeguarding and Data Protection Statement

Unloc.online and other forms of digital delivery (such as Google Meet, Zoom and Microsoft Teams) are designed to provide a safe online learning environment in line with Unloc's *Safeguarding and Child Protection Policy and Procedures* and Unloc's *Data Protection Policy and Procedures* which encompass all relevant UK and EU legislation and guidance.

Frequently Asked Questions

Q: Who can see what students are doing/typing? (Unloc.online)

A: This information is only viewable by Unloc staff, all of whom are appropriately trained and undergo Enhanced DBS Checks, and school/college staff as agreed by the main Point of Contact.

Q: What happens if a student types something that is a safeguarding concern? (Unloc.online)

A: Actions are taken in line with usual procedures including informing the school/college. All interactions with students are recorded and can be provided to a school/college if necessary.

Q: Where is students' information kept? (Unloc.online)

A: All information is kept on a secure third party provider with appropriate technical and organisational measures to ensure it is restricted to authorised personnel for the purposes of delivering services or business activities. We implement access controls, encryption measures & regular security checks.

Q: When will user data be deleted? (Unloc.online)

A: User accounts and their data are deleted once the user has decided they no longer wish to be a part of Unloc+ or by reaching out to the data protection officer.

Q: What controls are in place to keep students safe? (Google Meet, Microsoft Teams, Zoom)

A: Only people with a specific link can join the calls and waiting rooms are put in place. The Unloc staff member has the ability to remove or mute participants at any time. Students are reminded of good online etiquette at the start of every call including how to raise an issue directly with the Unloc staff member, how to control the sharing of their image/video, and how to avoid sharing personal information. Staff are never allowed to be in a digital room alone with a student. Young people are asked to ensure, where possible, that their name is changed on the online system to ensure safeguarding practices are followed.

If the session is being delivered on behalf of an educational institution, where possible, we will ask a staff member to be present to take lead on any safeguarding concerns. Where this cannot happen, the lead facilitator will obtain the contact details for the point of contact and/or safeguarding lead of the educational institution in case of an incident occurring or concern arising.