



22.01.2021

Fremdzugriff auf Videokonferenzen im Unterricht



Wichtige Hinweise für Lehrkräfte und Schulen

Aktuell gibt es den Trend, dass Schülerinnen und Schüler über Social-Media-Kanäle aufgefordert werden, fremden Personen (z.B. YouTuber) die Meetingdaten des Fernlernunterrichts weiterzugeben. Das bedeutet, fremde Personen bekommen die Login-URL mit Meetingraum und bei Live-Veranstaltungen zusätzlich das Passwort mitgeteilt. Die YouTuber/Fremden loggen sich dann in die Unterrichts-Konferenz ein, senden beleidigende Ausdrücke, sprechen die Lehrkräfte an, bzw. laden pornographisches Material hoch. Diese Aktion wird aufgezeichnet und dann z.B. in YouTube veröffentlicht, so dass dieser Vorfall weltweit verbreitet wird. Je größer die Klickzahl der Follower dann ist, umso mehr Geld verdient der YouTuber damit. Leider huldigen die Schüler oftmals den YouTuber noch als genialen Held, der als Störer im Unterricht so viel „Spaß“ verbreitet hat!

- Die Weitergabe von Passwörtern und Session IDs durch eigene Schüler ist durch die Nutzungsordnung verboten! Bitte sprechen Sie das vor jeder Videokonferenz noch einmal dringend an und sensibilisieren Sie Ihre Schülerschaft.
- Jede Videokonferenz muss maximal geschützt sein. Nutzen Sie bitte auch sogenannte Lobby- oder Warteräume der Software. (BBB ist durch die Authentifizierung über Moodle geschützt.)
- Nutzen Sie z.B. Jitsi nicht über den offenen Server *meet.jit.si*, sondern für den Unterricht ausschließlich mit den Angeboten der KMZ/SMZ/LMZ.
- Unerlaubte Aufzeichnungen von Videokonferenzen und die Verarbeitung von Bild und/oder Ton, bzw. die Veröffentlichung der Aufnahmen auf YouTube oder anderen Plattformen sind verboten und eine Verletzung der Persönlichkeitsrechte. Dies betrifft alle Beteiligten, Schüler/-innen wie Lehrkräfte! Ebenso sind dies Verstöße gegen den Datenschutz, das Urheberrecht und die informierte Selbstbestimmung. *Tipp: Strafgesetzbuch §303a ff. Datenveränderung - kann man mit den Schülern auch ansprechen!*
- Videokonferenzen sind nur ein Bestandteil des Fernlernunterricht. Sollten massive Störungen Ihre Konferenzen begleiten, dann brechen Sie diese ab und geben Aufgaben über alternative Wege an die Schüler/-innen weiter. Schulen sind nicht verpflichtet, nur Videokonferenzen als Fernlernunterricht durchzuführen.
- Massive Störungen sind zur Anzeige zu bringen. Werden personenbezogene Daten ohne Rechtsgrundlage weiterverarbeitet oder missbräuchlich genutzt, so handelt es sich nach Abwägung der Risiken auch um eine meldepflichtige Datenpanne nach Art. 33 DSGVO.
- Bitte sprechen Sie auch medienpädagogische Aspekte an! Der nun schon monatelange Einsatz von Lehrkräften und Schulleitungen für ihre Schülerschaft und im Endeffekt auch für die Eltern sollte doch durch diese unerträglichen Aktionen nicht demontiert werden.

Weitere und aktuelle Hinweise finden Sie wie gewohnt auf www.schulamt-karlsruhe.de im Artikel „Beratende Informationen zum Ersatzunterricht (Fernlernunterricht)“

Mit freundlichen Grüßen

Alexander Gnant

Staatliches Schulamt Karlsruhe
Ritterstraße 16-20
76133 Karlsruhe

E: alexander.gnant@ssa-ka.kv.bwl.de
E: datenschutz@ssa-ka.kv.bwl.de