Fremdzugriff auf Videokonferenzen im Unterricht

Wichtige Hinweise für Schulleitungen und Lehrkräfte

Aktuell gibt es leider den Trend, dass Schülerinnen und Schüler erfolgreich über Social-Media-Kanäle aufgefordert werden fremden Personen (z.B. sogenannte Youtuber) die Meeting Daten des Fernlernunterrichts weiterzugeben. Das bedeutet, fremde Personen bekommen die Login-URL mit Meeting-Raum und bei Live-Veranstaltungen zusätzlich das Passwort mitgeteilt.
Die Fremden loggen sich dann in die Unterrichtskonferenz ein. Dabei stören sie den Unterricht, sprechen Lehrkräfte an, senden Beleidigungen oder laden sogar pornografisches oder extremistisches Martial hoch. Diese Aktionen werden aufgezeichnet und dann in Youtube veröffentlicht, so dass dieser Vorfall einer unbegrenzten Personenmenge zur Verfügung gestellt und weltweit verbreitet werden kann.
Je größer die Klickzahl der Follower ist, umso mehr Geld verdient der Youtuber damit. Leider wird so ein Youtuber dann noch für seine Taten als Held gefeiert, da er als Störer im Unterricht viel „Spaß" verbreitet hat. Allerdings hat so eine Aktion mit Spaß nichts zu tun.

Daher sind folgende Punkte unbedingt zu beachten:

- Die Weitergabe von Passwörtern und Session-IDs durch eigene Schülerinnen und Schüler ist durch die Nutzungsordnung verboten. Bitte sprechen Sie das vor jeder Videokonferenz noch einmal dringend an und sensibilisieren Sie die Schüler.
- Jede Videokonferenz muss maximal geschützt werden. Fall möglich, nutzen Sie sogenannte Lobby- oder Warteräume der Software. Gewähren Sie nur bekannten Schülerinnen und Schülern Zutritt zu dem Konferenzraum (Bei BigBlueButton über Moodle ist die Authentifizierung über Moodle geregelt).
- Andere Videosoftware wie z.B. Jitsi soll für den Unterricht nur über die Angebote der Medienzentren KMS, LMZ, SMZ, Hopp-Foundation genutzt werden. Freie und damit offene Jitsi Server sollen nicht genutzt werden.
- Unerlaubte Aufzeichnungen von Videokonferenzen und die Verarbeitung von Bild und/oder Ton bzw. deren Veröffentlichung auf Youtube oder jeder anderen Plattform sind verboten und eine Verletzung der Persönlichkeitsrechte. Die betrifft alle Beteiligten, sowohl Schülerinnen und Schüler als auch Lehrkräfte. Ebenso stellt dies ein Verstoß gegen den Datenschutz, das Urheberrecht und die informierte Selbstbestimmung dar.
- Videokonferenzen sind nur ein Bestandteil des Fernlernunterrichts. Sollten Sie solche massiven Störungen feststellen, können Sie den Videounterricht sofort abbrechen und unterrichten Sie auf alternative Weise. Auch die Aufgabenübermittlung kann auf alternativem Weg an die Schüler erfolgen. Die Schulen sind nicht verpflichtet den Fernlernunterricht nur über Videokonferenzen zu realisieren.
- Die Störung des Unterrichts birgt auch eine strafrechtliche Relevanznach dem Strafgesetzbuch. Von daher sollte jede Störung des Unterrichts zur Anzeige gebracht werden.
- Werden personenbezogene Daten ohne Rechtsgrundlage weiterverarbeitet oder missbräuchlich genutzt, so handelt es sich unter Umständen nach Abwägung des Risikos um eine meldepflichtige Datenpanne nach Art. 33 DSGVO. Bitte nehmen Sie in diesem Falle auch Kontakt mit Ihrem Datenschutzbeauftragten auf.
- Bitte sprechen Sie auch medienpädagogische Aspekte an. Der nun schon monatelange beachtliche Einsatz von Lehrkräften und Schulleitungen für die Schüler sollte durch solche unerträglichen Aktionen nicht demontiert werden.

Weitere Hinweise können Sie beiliegendem Hinweisblatt des Kultusministeriums in Zusammenarbeit mit dem Landeskriminalamt zur Nutzung von Videosoftware durch Schulen entnehmen.

gez.
Datenschutzbeauftragte des
Staatlichen Schulamts Mannheim