Hessisches Kultusministerium

HESSEN

Hessisches Kultusministerium Postfach 3160 65021 Wiesbaden

An die
Schulleiterinnen und Schulleiter
der hessischen Schulen

über
die jeweils zuständigen
Staatlichen Schulämter

Geschäftszeichen 540.042.020-00350
Bearbeiter Dr. Jeck
Durchwahl 0611 368 2718

Ihr Zeichen
Ihre Nachricht

Datum 28. Januar 2021

Störungen und Missbrauch von Videokonferenzen

hier: Rechtliche, polizeiliche und psychologische Handlungsempfehlungen

Sehr geehrte Schulleiterinnen und Schulleiter,

von vielen Lehrerinnen und Lehrern werden derzeit zur Kommunikation mit Schülerinnen und Schülern Videokonferenzsysteme im digitalen Distanzunterricht verwendet.
Bereits im letzten Jahr hatten wir darauf hingewiesen, dass in dem Eindringen unerwünschter Personen in die virtuellen Besprechungen, dem sogenannten „Zoombombing", eines der größten Risiken neben der Verletzung des Datenschutzes beim Einsatz von Videokonferenzsystemen besteht. Störende können die Gelegenheit nutzen, um z.B. pornografisches Material, rassistische oder antisemitische Ansichten zu verbreiten.
Aktuell häufen sich Vorfälle dieser Art, zuletzt wurden z.B. Grundschülerinnen und Grundschüler plötzlich während des digitalen Unterrichts mit pornografischen Videos konfrontiert und Lehrkräfte beleidigt. In beiden Fällen hatten sich fremde Personen unbefugt Zugang zur Videokonferenz verschafft. Dies führt zu einer großen Verunsicherung in den Schulen, bei den Schülerinnen und Schülern und den Eltern.
Aus diesem Grund möchten wir Ihnen nachfolgende Informationen zur Verfügung stellen, um mit derlei Situationen und plötzlichen Störfällen sensibel im schulischen Alltag umgehen zu können.
Neben den u.a. vom Hessischen Landeskriminalamt und dem Hessen Cyber Competence Center (Hessen3C)(s.u.) stammenden Handlungsempfehlungen, die wir Ihnen nachfolgend geben möchten, gelten weiterhin die Hinweise, die Ihnen aus den Informationsschreiben des vergangenen Jahres bekannt sind.[1] Hierin wurden Sie über den Einsatz von Videokonferenzsystemen im schulischen Alltag informiert und darauf hingewiesen, dass es innerhalb der Schule ein abgestimmtes Vorgehen dahingehend,

[1] „Hinweise zu den organisatorischen und rechtlichen Rahmenbedingungen zu Beginn der Unterrichtszeit im Schuljahr 2020/2021" vom 23. Juli 2020 und „Einsatz digitaler Werkzeuge im Schulalltag" vom 20. August 2020

Luisenplatz 10, 65185 Wiesbaden
Telefon (0611)368-0 Telefax (0611)368-2099

E-Mail: poststelle.hkm@kultus.hessen.de
Internet: www.kultusministerium.hessen.de

welches Videokonferenztool unter Beachtung der datenschutzrechtlichen[2] und sicherheitsrelevanten[3] Vorgaben genutzt wird, geben sollte.

1. Technischer Schutz vor Fremdzugriffen und Sicherheitsvorkehrungen

Auch wenn kein hundertprozentiger technischer Schutz vor sogenannten Hackern und Trollen möglich ist, gibt es Maßnahmen, mit denen sich das Risiko unautorisierter Zugriffe minimieren lässt. Entscheidend ist hierbei vor allem der Konferenzzugang. Bei den meisten Lösungen erstellt die Lehrkraft einen sog. Konferenzraum und verschickt hierzu Einladungen oder Meeting-IDs. Es kann von Vorteil sein, diese Zugänge über einen längeren Zeitraum unverändert zu lassen, um den Schülerinnen und Schülern den Zugang zu erleichtern. Gleichzeitig liegt hierin aber ein beträchtliches Sicherheitsrisiko. Diese Zugänge sollten niemals öffentlich verteilt oder kommuniziert werden. Die Schülerinnen und Schüler müssen deshalb sensibilisiert werden, mit diesen Zugängen entsprechend vorsichtig und verantwortungsvoll umzugehen. Die Lehrkraft sollte außerdem zu jeder Zeit die Kontrolle über den Zugang zur Videokonferenz haben. Hierzu eignen sich Maßnahmen wie z.B. das Vergeben eines Passwortes oder einer PIN oder auch das Einrichten von Zugangsräumen, über die dann die Teilnehmerinnen und Teilnehmer erst zugelassen werden, wenn man sie eindeutig identifizieren kann.
Die Lehrkraft sollte während der Videokonferenz sicherstellen, dass sie in der Lage ist, Teilnehmende oder unerwünschte Inhalte aus der Konferenz zu entfernen. Konferenzsysteme, in denen es keine explizite Rolle als Administrator/-in für die Lehrkraft gibt, sind nicht zu empfehlen!
Falls Sie hierzu Unterstützung benötigen, stehen Ihnen die Fachberatungen für Medienbildung an den Staatlichen Schulämtern und die regionalen Medienzentren als mögliche Anlaufstellen zur Verfügung.

Um mehr Sicherheit im Umgang mit Videokonferenzsystemen zu gewinnen, bietet die Lehrkräfteakademie Lehrerinnen und Lehrern verschiedene Online-Fortbildungen an, die auch die Vermeidung potentiellen Missbrauchs zum Inhalt haben.
Darüber hinaus steht Lehrkräften auch das e-Learning-Angebot „Grundlagenwissen zur Informationssicherheit" von Hessen3C zur Verfügung (siehe Anlage).

Außerdem sind folgende grundsätzliche Vorkehrungen gemäß Hessen3C zu empfehlen:

- Um auf Sicherheitsvorfälle adäquat reagieren zu können, sind schulinterne Meldeketten einzurichten.
    - Meldungen haben unverzüglich zu erfolgen.
    - Die Schulleitung ist zu informieren und im Fall von Videokonferenzsystemen, die durch den Schulträger betrieben werden, ebenso der/die Informationssicherheitsbeauftragte und der/die Datenschutzbeauftragte des Schulträgers.

---

[2] Orientierungshilfe Videokonferenzsysteme und Checkliste Datenschutz in Videokonferenzsystemen (siehe Homepage des Hessischen Beauftragten für Datenschutz und Informationsfreiheit)

[3] Siehe Kompendium Videokonferenzsysteme des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

- Um im Klassenverband zeitnah auf entsprechende Vorfälle reagieren zu können, wird empfohlen, einen einheitlichen E-Mail-Verteiler der jeweiligen Klasse durch die Klassenlehrkraft einzurichten und diesen stets aktuell zu halten. Der Versand von E-Mails durch Lehrkräfte darf ausschließlich über E-Mail-Adressen des Landes oder der Schulträger erfolgen. Darüber hinaus können an der Schule alternative Kommunikationswege genutzt werden (z.B. Schulportal, externe Lernplattform, datenschutzkonformer Messengerdienst).
- Es wird empfohlen, für den Online-Unterricht einen geschlossenen Teilnehmerkreis zu nutzen und die Benutzernamen der Schülerinnen und Schüler so festzulegen, dass eine eindeutige Identifikation des jeweiligen Gruppenmitglieds möglich ist. Unberechtigte können so schnell identifiziert und aus dem Meeting entfernt werden.
- Die Teilnehmenden sollten darauf hingewiesen werden, dass die zur Einwahl in den Onlineunterricht verwendeten mobilen Endgeräte vor einem unberechtigten Zugriff geschützt sein müssen. Bei einer Abwesenheit sollten die Teilnehmenden dahingehend sensibilisiert werden, dass sie ihre mobilen Geräte sperren.

2. Verhaltensregeln beim Einsatz eines virtuellen Konferenzraums

Vor der Durchführung einer Videokonferenz sollten Lehrkräfte Verhaltensregeln mit den Schülerinnen und Schülern besprechen. Neben den allgemeinen Verhaltensregeln für ein strukturiertes Kommunizieren, die auch außerhalb einer Videokonferenz gelten, gibt es bei Videokonferenzen noch einige zusätzliche Punkte zu beachten:

- Das Teilen von unangemessenen Inhalten ist verboten. Im schlimmsten Fall (bei Aufnahmen sexualisierter Gewalt an Kindern, Antisemitismus etc.) stellt die Speicherung und Verbreitung eine Straftat dar.
- Passwörter bzw. Pin-Codes und Zugänge (Einladungslinks) sind vertraulich zu behandeln und seitens der Lehrkraft möglichst getrennt zur Verfügung zu stellen.
- Schülerinnen und Schüler sollten keine Moderatorenrechte für den Konferenzraum erhalten.
- Die Bildschirmfreigabe sollte grundsätzlich deaktiviert sein und nur durch die Lehrkraft freigegeben werden können.
- Private Chatmöglichkeiten sollten, wenn möglich, deaktiviert werden.
- Die Lehrkraft sollte nach Ende der Unterrichtseinheit die Konferenz nicht einfach verlassen, sondern sie beenden, damit die Schülerinnen und Schüler nicht unbeaufsichtigt im Konferenzraum bleiben können.

3. Vorgehen bei einer Störung und Meldung eines Vorfalls

Sofern es trotz der vorgenannten Maßnahmen zu einem Zwischenfall und einer schwerwiegenden Störung kommen sollte, wird auch seitens der Polizei folgendes Vorgehen empfohlen:

- Sofern es sich um strafrechtlich relevante Sachverhalte handelt, sollten umgehend Screenshots zur Beweissicherung angefertigt werden und Anzeige bei der zuständigen Polizeidienststelle erstattet werden.

- Entfernen Sie grundsätzlich nicht eingeladene Personen aus dem Meeting.
- Beenden Sie bei Zwischenfällen mit Schülerinnen und Schülern die Sitzung umgehend und stellen Sie neue Zugangsdaten mit einem neuen Passwort zur Verfügung.
- Melden Sie Sicherheitsvorfälle unverzüglich auf dem vom Schulträger vorgegebenen Weg.
- Informieren Sie außerdem unmittelbar das Staatliche Schulamt und im Anschluss die betroffenen Eltern. Bitte bieten Sie den Eltern bei Bedarf professionelle Unterstützung an (siehe Nr. 4).

4. Polizeiliche und psychologische Unterstützung im Ereignisfall

Im Bereich der kriminalpolizeilichen Prävention stehen in jedem Polizeipräsidium Ansprechpersonen für die Bereiche Jugendkoordination, Prävention Cybercrime und Opferschutz für entsprechende Beratungen bei einem Vorfall zur Verfügungen. Die Übersicht aller Ansprechpersonen ist auf www.polizei.hessen.de eingestellt.

Das Hessen Cyber Competence Center (Hessen3C) im Hessischen Ministerium des Innern und für Sport berät die Schulträger in allen Fragen der IT-Sicherheit und unterstützt bei Sicherheitsvorfällen.
Zum kostenlosen Leistungsangebot gehören

- IT-Sicherheits-Prozess- und Architektur-Beratung
- Unterstützung bei Sicherheitsvorfällen: 24/7-Hotline unter 0611-353-9900
- Anlassbezogene Awareness-Veranstaltungen für Schulleitungen und Lehrkräfte

Auch wenn die Täterinnen und Täter (häufig männliche Jugendliche und junge Erwachsene) mit ihrem Vorgehen demonstrieren, dass sie in der Lage sind, die Kontrolle über eine Videokonferenz zu übernehmen, und mit den gezeigten Inhalten bewusst schockieren und Grenzen verletzen wollen, bedeutet dies nicht per se, dass davon betroffene Schülerinnen und Schüler oder Lehrkräfte in einer solchen Situation traumatisiert werden. Abhängig vom Alter der Kinder und Jugendlichen, ihren Vorerfahrungen und ihrem Verständnis des gezeigten problematischen Inhalts, kann es sehr unterschiedliche Reaktionen geben. In den meisten Fällen werden die Kinder und Jugendlichen die Situation ohne psychische Folgeschäden bewältigen. Die eher seltene, aber vorhandene Gefahr einer Re-Traumatisierung nach einer Vorführung gewalthaltiger und verstörender Inhalte besteht insbesondere bei Personen, die die gezeigte Gewalt selbst einmal erlebt haben.
Betroffene Eltern und Lehrkräfte sollten deshalb versuchen, Rückmeldungen und emotionales Belastungserleben der Kinder und Jugendlichen genau wahrzunehmen, und verständnisvoll darauf reagieren.
Bei Bedarf kann es erforderlich sein, die Thematik in pädagogisch geeigneter Art und Weise mit den Schülerinnen und Schülern im Unterricht zu erörtern oder sich zusätzliche psychologische Unterstützung zu holen. In diesen Fällen stehen z.B. die Schulpsychologinnen und Schulpsychologen der Staatlichen Schulämter den Lehrkräften und Eltern sowie den Schülerinnen und Schülern für Beratung und professionelle Unterstützung vor Ort zur Verfügung.

5. Weitergehende Informationen

Neben der HKM-Handreichung zum Jugendmedienschutz (https://kultusministerium.hessen.de/foerderangebote/medienbildung/jugendmedienschutz) können Ihnen, falls noch nicht bekannt, die folgenden Broschüren weitergehende Handlungsempfehlungen geben:

- Sicherheit im Medienalltag: SCHULE FRAGT. POLIZEI ANTWORTET. (Eine Handreichung für Lehrerinnen und Lehrer)
- Medienpädagogische Arbeitshilfe zur Reihe „Ethik macht klick“ von klicksafe.de „Baustein 2 - Verletzendes Online-Verhalten“

Zusätzlich finden Sie als Anlagen

- den Flyer des Netzwerks gegen Gewalt zur Medienkompetenz für Eltern und
- ein Musterinformationsschreiben für Eltern.

Wir wünschen Ihnen, dass Sie im Schulalltag mit entsprechenden Vorfällen möglichst nicht konfrontiert werden. Sollten Sie doch einmal von einer Störung durch Dritte betroffen sein, können Ihnen unsere Hinweise hoffentlich eine Unterstützung im Sinne einer angemessenen Reaktion sein. Zögern Sie bitte nicht, im Bedarfsfall eine der genannten Kontaktadressen anzusprechen und professionelle Hilfe in Anspruch zu nehmen.

Für die Durchführung Ihres Distanzunterrichts wünschen wir Ihnen weiterhin viel Erfolg!

Mit freundlichen Grüßen
Im Auftrag

Wolf Schwarz
Ministerialdirigent
Abteilungsleiter I

Mit freundlichen Grüße
Im Auftrag

Jörg Meyer-Scholten
Ministerialdirigent
Abteilungsleiter Z