# Hinweisschreiben Umgang mit Videokonferenzsystemen

Sehr geehrte Damen und Herren,
liebe Eltern und Erziehungsberechtigte,

aufgrund der anhaltenden Pandemielage werden im Schulbetrieb zur Durchführung des Unterrichts teilweise Videokonferenzsysteme eingesetzt. Durch den vermehrten Einsatz dieser Konferenzsysteme, stieg auch die Anzahl der Probleme und Störungen. In einigen Fällen haben sich unbekannte Personen Zutritt zu Videokonferenzen verschafft und diese dann missbraucht (sogenanntes „Zoombombing"). Dies geschieht meist dadurch, dass Unbefugte typische Konferenzkennungen oder häufiger genutzte Passwörter erraten, um sich einzuwählen. Eine weitere Möglichkeit für solche unautorisierten Zugriffe besteht darin, dass Konferenzkennungen bewusst an Dritte weitergegeben oder über Soziale Medien verbreitet werden, um einen geregelten Unterricht zu verhindern.

Wie schwerwiegend ein solcher Vorfall sein kann, hängt von der verwendeten Konferenzsoftware ab. Die Friedrich-Magnus-Gesamtschule verwendet für die Konferenzen das entsprechende Modul von IServ, welches auf der Software BigBlueButton basiert. BigBlueButton hat ein Rechtesystem, bei dem Moderatoren (Lehrer) eine relativ gute Kontrolle über die Konferenzen haben. Ein Teilnehmer kann bei BigBlueButton nicht die Ersteller oder Moderatoren aus der Konferenz entfernen und sich die administrativen Rechte über die Konferenz aneignen, wie es bei einigen anderen Lösungen der Fall ist.

Außerdem können unsere Konferenzen in der Regel nur von Schülerinnen und Schülern genutzt werden, die über eine IServ-Anmeldung unserer Schule verfügen. Die Lehrkraft sieht somit in der Konferenz die Namen von jedem einzelnen Teilnehmer und kann die Rechte einschränken oder die Person aus der Konferenz ausschließen. Insgesamt kann das Gefahrenpotential für unsere IServ-Lösung als relativ gering eingeschätzt werden.

Auch wenn seitens der Schule alle möglichen Vorkehrungen getroffen werden, lassen sich vermutlich nicht alle Probleme vollständig vermeiden.

Daher möchten wir Sie in diesem Zusammenhang nochmals auf den Umgang mit Videokonferenzsystem aufmerksam machen und Sie bitten, auch ihr Kind hierfür zu sensibilisieren. Unterstützen Sie uns dabei, die Videokonferenzen so sicher wie möglich durchzuführen.

Insbesondere bitten wir Sie folgende Punkte zu beachten:

- Konferenzkennungen, sowie Passwörter für persönliche Anmeldungen dürfen nicht an unbefugte Dritte weitergegeben und insbesondere nicht auf Sozialen Medien veröffentlicht werden.
- Eine Aufzeichnung oder Übertragung des Unterrichts an Dritte darf nicht erfolgen. Ein solches Verhalten kann gemäß § 201 Strafgesetzbuch strafbar sein.
- 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.
- Während des Distanzunterrichts mittels Videokonferenzsystemen sollte darauf geachtet werden, dass die Schülerinnen und Schüler keine sensiblen persönlichen Informationen von sich oder Dritten preisgeben.
- Die Schülerinnen und Schüler sollten angehalten werden, sich bei verdächtigen Vorkommnissen unverzüglich an die Lehrkräfte und/oder Eltern zu wenden. Auf die Möglichkeit, strafrechtliche Schritte einzuleiten (beispielsweise Strafanzeige zu stellen), wird hingewiesen.
- Bei Bedarf kann schulpsychologische Hilfe in Anspruch genommen werden.

Abschließend möchten wir auf die Handreichung des Hessischen Kultusministeriums zum Jugendmedienschutz sowie auf den Flyer des Netzwerks gegen Gewalt: Medienkompetenz für Eltern hinweisen:

https://kultusministerium.hessen.de/foerderangebote/medienbildung/jugendmedienschutz

Wir wünschen Ihnen, dass Sie und Ihr Kind im Schulalltag mit entsprechenden Vorfällen möglichst nicht konfrontiert werden. Zögern Sie bitte nicht, im Bedarfsfall eine der genannten Kontaktadressen zu nutzen und professionelle Hilfe in Anspruch zu nehmen.

Mit freundlichen Grüßen

Irina Reh
Schulleiterin