POLIZEIINSPEKTION
STADE

Informationsbrief Ihres Beauftragten für Jugendsachen

Beiblatt „Absicherung von Videokonferenzen“

Diese Informationen dienen als Empfehlung für ein sicheres und produktives virtuelles Klassenzimmer – aber auch für Videokonferenzen in anderen Zusammenhängen…

- ***Kennwort erforderlich:*** Erstellen Sie ein Meeting- oder Webinar-Kennwort und teilen Sie es nur mit Lernenden/Teilnehmenden, um sicherzustellen, dass nur Gäste mit dem Kennwort Ihr virtuelles Klassenzimmer/Ihre Videokonferenz betreten können. Das Versenden des Passwortes in einer gesonderten E-Mail erhöht die Sicherheit. Bei der Nutzung von IServ bleibt es erforderlich, die Anwesenheit der Teilnehmenden zu überprüfen und auf nicht legitimierte Nutzer- /innen entsprechend zu reagieren. *Das virtuelle Klassenzimmer bleibt ein Klassenzimmer – so wie in der Schule. Der Zugang ist nur für Berechtigte möglich.*

- ***Warteräume aktivieren:*** Warteräume verhindern, dass Teilnehmende automatisch einem Meeting beitreten. Sie können jeden Teilnehmenden einzeln zulassen oder (nach Prüfung) alle auf einmal. Sie können auch Lernenden / Teilnehmenden, die über die Domäne Ihrer Schule angemeldet sind, erlauben, den Warteraum zu überspringen, während Teilnehmende, die nicht Teil der Domäne Ihrer Schule sind, einzeln zugelassen werden müssen.

  Warteräume ermöglichen das Führen einer Anwesenheitsliste –
  so wie die analoge Anwesenheitsüberprüfung im Klassenbuch.

- ***Bildschirmfreigabe deaktivieren:*** Nur der Host (Gastgeber/ Moderator/ Präsentator) sollte seinen / ihren Bildschirm teilen können. So wird verhindert, dass Teilnehmende unerwünschte oder ablenkende Inhalte teilen. Damit Teilnehmende Inhalte teilen können, können Sie diese Einstellung individuell und im Bedarfsfall anpassen oder das Teilen während des Meetings im Einzelfall aktivieren. Eine klare Struktur der Rollen und den jeweils hinterlegten Berechtigungen ist sinnvoll. *Beiträge und Wortmeldungen sollten behandelt werden wie im Präsenzunterricht. Wer etwas beizutragen hat, macht auf sich aufmerksam, wird gezielt aufgefordert sich zu beteiligen, oder „meldet“ sich über den Chat.*

- ***Privaten Chat deaktivieren:*** Der Host kann den Chat sperren, bzw. nach eigenen Bedürfnisse einstellen. Es kann also vom Host entschieden werden, welche Chatmöglichkeiten „offen“ sind. So können z.B. alle Teilnehmenden private Nachrichten an alle schreiben, oder nur an den Gastgeber.

- ***Teilnehmende verwalten***: Wenn ein ungebetener Gast an Ihrem Unterricht / Meeting teilnimmt, können Sie diesen Teilnehmenden entfernen. Weitere Informationen zur Verwaltung von Teilnehmenden, wie die Möglichkeit, diese stummzuschalten, deren Video auszuschalten und Umbenennungen einzuschränken, sind von Anbieter zu Anbieter verschieden. Nähere Informationen erhalten Sie in der Regel vom jeweiligen Support-Center. Die sichere Bedienung und der versierte Umgang durch den Host sollten vor Beginn der Videokonferenz sichergestellt sein.

- ***Meeting sperren:*** Sie können auch das Meeting sperren, um zu verhindern, dass andere Teilnehmende dem Meeting nach Beginn beitreten. Mit dieser Funktion werden nicht nur ungebetene Gäste von der Teilnahme abgehalten, sondern es kann auch sichergestellt werden, dass niemand zu spät kommt.

- ***Klarnamen-Pflicht:*** Vermeintliche Anonymität fördert abweichendes Verhalten und begünstigt eine ungewollte Entwicklung. Deshalb ist eine Klarnamen-Pflicht sinnhaft.

- ***Technisches Know-how:*** Das Anfertigen von Bildschirmfotos beispielsweise kann der Beweisaufnahme und somit der etwaigen Strafverfolgung nutzen.

Der versierte Umgang mit den unterschiedlichen Endgeräten und Anwendungen muss gewährleistet sein.

- ***Schutz der Privatsphäre:*** Stellen Sie sicher, dass im Hintergrund keine persönlichen Gegenstände (wie zum Beispiel private Fotos) zu sehen sind. Die Nutzung von einem Headset kann dazu beitragen, dass Inhalte ausschließlich den Empfänger erreichen und nicht ungewollt Andere mithören.

- ***Klare Regeln:*** Es kann hilfreich sein, zum Beginn eines Meetings die Grundregeln zu wiederholen. Insbesondere das Verbot nicht legitimierter Aufzeichnungen von Meetinginhalten muss angesprochen werden. Dass die Weitergabe vom Zugangslinks und Passwörtern an Unberechtigte nicht erlaubt ist, muss allen Teilnehmenden bewusst sein.

„Virtuelle Klassenzimmer“ - bleiben Klassenzimmer. „Virtuelle Besprechungsräume“ - bleiben Besprechungsräume. Der stetige Vergleich bietet sich an.

Diese Regeln erheben keinen Anspruch auf Vollständigkeit. Sie basieren auf den Ausführungen und Tipps von www.klicksafe.de und dem Support-Blog des Anbieters Zoom. Die ausschließliche Nutzung von IServ über die personengebundenen Zugänge ist ein guter Weg, ein sicheres „virtuelles Klassenzimmer“ zu besuchen. Grundsätzlich gelten die oben aufgeführten Regeln auch dort. Sie sind nur nicht immer technisch umsetzbar. Den Hinweis auf den IServ-News Feed „Informationen zum Schutz vor Videokonferenzmissbrauch“ führe ich hier ergänzend mit auf.