POLIZEIINSPEKTION
GÖTTINGEN

Informationsbrief Ihrer 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) 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 oder wird gezielt aufgefordert, sich zu beteiligen.

- Privaten Chat deaktivieren: Der Host kann den Chat sperren, damit Teilnehmende private Nachrichten in diesem Chat nicht austauschen können. Teilnehmende können aber weiterhin mit dem Host chatten.

- 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, die Videoübertragung 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. Bei IServ ist dies gewährleistet.

- 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 von 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, dem Support-Blog des Anbieters Zoom und fachlicher Beratung. 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.

POLIZEIINSPEKTION
GÖTTINGEN

Informationsbrief Ihrer Beauftragten für Jugendsachen

der Polizeiinspektion Göttingen

Sehr geehrte Eltern und Erziehungsverantwortliche, liebe Lehrerinnen und Lehrer,

in den letzten Tagen und Wochen wurde über diverse Vorfälle im Zusammenhang mit Videokonferenzen medial berichtet. Inzwischen gibt es dafür sogar einen Begriff: „Zoombombing". Dieses Phänomen ist hier im Bereich der Stadt und dem Landkreis Göttingen bisher noch nicht aufgetreten, dennoch möchte ich die polizeilich bekannten Fälle aus Lüneburg zum Anlass nehmen, Ihnen ein paar Tipps und Hinweise an die Hand zu geben.

Beim so genannten „Zoombombing" verschaffen sich Unberechtigte Zugang zu Videokonferenzen und stören diese durch unsachliche Kommentare, Eingriffe in die Administration der Konferenz und auch durch das Teilen von unerwünschten, abstoßenden und zum Teil rechtswidrigen Inhalten wie Pornografie, Verherrlichung von Gewalt oder rassistischen und antisemitische Ansichten.

Diese Vorfälle sind ebenfalls im Zusammenhang mit dem Lernen auf Distanz im schulischen Kontext bekannt geworden.

Auch wenn Anbieter wie Zoom ihre Sicherheitsvorkehrungen verstärkt haben, bleibt ein Restrisiko bestehen.

Die Schule soll ein Ort der Sicherheit, der Verlässlichkeit und des Vertrauens sein. Diesem Anspruch müssen auch digitale Lern- und Lehrkonzepte gerecht werden können.

Die Sicherheit der Schülerinnen und Schüler beim digitalen Schulbesuch zu gewährleisten und Straftaten in deren Lebensraum zu verhüten, muss das gemeinsame Ziel sein. Zudem muss die Entscheidung von Schülerinnen und Schülern zu gesetzestreuem und prosozialem Verhalten auch außerhalb der Schule gestärkt werden.

Ich möchte Sie motivieren, mit Ihren Kindern / Ihrem Kind sowie Ihren Schülerinnen und Schülern folgende Aspekte und Verhaltensregeln zu thematisieren:

- Digitales Lernen kann nur gelingen und Spaß machen, wenn grundlegende Verhaltensregeln eingehalten werden und der respektvolle, wertschätzende Umgang miteinander beachtet wird.
- Dabei muss der rechtliche Rahmen eindeutig kommuniziert und bekannt sein. Das Internet ist kein regel- oder rechtsfreier Raum. Die Verhaltensregeln und Gesetze lassen sich ohne Abstriche aus dem „echten Leben" übertragen.
- Das „digitale Klassenzimmer" sollte wie ein Klassenzimmer in der Schule betrachtet werden. Es gelten die entsprechenden Regeln und zivil- bzw. strafrechtlichen Gesetze.
- Ein besonderes Augenmerk liegt im Bereich des prosozialen Mitwirkens bei Online-Lehrveranstaltungen, um den gemeinsamen Lernerfolg unter diesen ohnehin herausfordernden Bedingungen zu ermöglichen.
- Das Bewusstsein und ein Verständnis dafür, welche Inhalte zivil- und strafrechtlich relevant sein können und daher unter keinen Umständen geteilt werden dürfen, ist besonders wichtig.

Dieses Verständnis und das moralische Bewusstsein zu schaffen, liegt in unser aller Verantwortung.

POLIZEIINSPEKTION
GÖTTINGEN

Exemplarisch sollen folgende Beispiele die mögliche Tragweite verdeutlichen:

- Das Beleidigen von Mitschüler- /innen oder Lehrkräften kann den Tatbestand des § 185 StGB erfüllen.
- Über eine Person wissentlich Unwahrheiten zu verbreiten, diese verächtlich zu machen, in der öffentlichen Meinung herabzuwürdigen oder öffentlich zu verunglimpfen, kann den Tatbestand der Üblen Nachrede gemäß § 186 StGB bzw. der Verleumdung gemäß § 187 StGB erfüllen.
- Das Bild einer Person ohne deren Einverständnis in Chats oder auf sonstigen Plattformen zu veröffentlichen, stellt einen Verstoß gegen das Kunsturheberrecht dar.
- Die nicht legitimierte Aufzeichnung von Bild / Video und Ton in virtuellen Klassenräumen sowie deren Veröffentlichung stellt eine Straftat im Sinne des § 201 StGB (Verletzung der Vertraulichkeit des Wortes) dar.
- Das Teilen von pornografischen Inhalten, obszönen, gewaltverherrlichenden, antisemitischen, fremdenfeindlichen oder volksverhetzenden Inhalten kann ebenfalls einen Straftatbestand darstellen. Teilweise ist bereits der Besitz strafbar.
- Das Weitergeben von Passwörtern und Zugangsberechtigungen oder das regelwidrige Erschleichen dieser Daten kann ebenfalls zu einer Strafanzeige führen.

Dies sind nur einige Beispiele dafür, dass ein Fehlverhalten in der digitalen Welt strafrechtliche Konsequenzen haben kann. Die Schulen sind gehalten, strafrechtlich relevantes Verhalten im Schulkontext der Polizei zu melden. Dies kann wiederum polizeiliche Ermittlungen nach sich ziehen. Als Eltern steht es Ihnen frei, derartige Vorkommnisse der Polizei zu melden. Eine Anzeige können Sie jederzeit bei Ihrer Polizeidienststelle vor Ort erstatten. Diese Anzeige ist an keine Form gebunden. Bei uns in Niedersachsen können Sie eine Anzeige auch über die Online-Wache (www.onlinewache.polizei.niedersachsen.de) stellen. Das ist auch möglich, wenn eine Tat bereits längere Zeit zurückliegt. Bitte beachten Sie unbedingt, dass zum Beispiel IP-Adressen und Verbindungsdaten nur eine sehr begrenzte Zeit bei den Anbietern gespeichert sind.

Aus dem schulischen Kontext wurde mir darüber hinaus zugetragen, das Schülerinnen und Schüler während des Fernunterrichts – in der Regel über die Plattform IServ – parallel auf anderen Kanälen miteinander kommunizieren. Diese Kommunikationswege liegen dann außerhalb des Einflussbereiches der Lehrkraft. Für diese Kommunikation werden zum Beispiel WhatsApp oder Discord genutzt. Gerade auf diesem Wege werden unangemessene Inhalte verbreitet und Straftaten begangen. Das aktive Verfolgen des Unterrichtes wird darunter ebenfalls erheblich leiden. Bitte haben Sie auch diese „Parallelkommunikation" kritisch im Auge.

Tipps für den sicheren Umgang mit Videokonferenzen finden Sie bei Interesse auf dem Beiblatt

Für Fragen oder bei weitergehendem Beratungsbedarf können Sie mich gern kontaktieren.

KOK'in Corinna Klaus-Rosenthal – Beauftragte für Jugendsachen
Email: corinna.klaus-rosenthal@polizei.niedersachsen.de
Telefon: 0551/ 491-2008