

Zoom-Checkliste für Lehrer

basierend auf der Orientierungshilfe

des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

vom 28. Januar 2021

V 1.00

(21.04.2021)



Hinweis zur Nutzung dieses Dokuments

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat am 28. Januar 2021 eine [Orientierungshilfe zum Datenschutz bei Videokonferenzsystemen für Schulen](#) veröffentlicht.

Zoom begrüßt die Orientierungshilfe, da sie Schulen beim sicheren Betrieb von Videokonferenzsystemen hilft.

Um es Zoom-Kunden so einfach wie möglich zu machen, die Orientierungshilfe umzusetzen, veröffentlichen wir dieses Dokument. In der linken Spalte finden Sie die Kriterien der Orientierungshilfe, die wir unverändert übernommen haben. Auf der rechten Seite finden Sie Hinweise von Zoom zu den Einstellungsmöglichkeiten und weiterführenden Informationen.

Bitte beachten Sie, dass Zoom mit diesem Dokument keinerlei Rechtsberatung anbietet oder rechtliche verbindliche Erklärung abgibt. Dieses Dokument dient ausschließlich zu Informationszwecken.

Wir hoffen, dass Ihnen dieser Zoom-Leitfaden hilft und freuen uns über Ihr Feedback.

Einladung zu den Videokonferenzen

Orientierungshilfe	Zoom-Kommentar
<ul style="list-style-type: none"> Einladungs-Links oder Meeting-IDs sollten niemals auf der Homepage der Schule veröffentlicht, oder über soziale Netzwerke an die Schülerinnen und Schüler verteilt werden. 	<ul style="list-style-type: none"> Zusätzlich zu diesen wichtigen Schutzmaßnahmen, die vom Einladenden vorgenommen werden müssen, stellt Zoom einen “At Risk Meeting Notifier” zu Verfügung. Der Notifier scannt öffentliche Webseiten und Social Media-Inhalte bezüglich eingestellter Links zu Zoom Meetings (also Links zu Meetings, die eine Zoom-URL enthalten). Wird eine solche URL gefunden, informiert Zoom den Account-Owner. Zoom hat bis heute über 100.000 E-Mails an Account-Owner versendet, um sie vor möglichen Problemen mit ihren Meetings zu warnen.

2. Zutrittskontrolle – Wer darf in die Konferenz?

Orientierungshilfe	Zoom-Kommentar
<p>Passwörter: Das verwendete Videokonferenzsystem sollte die Möglichkeit bieten, die einzelnen Konferenzen mit einem Passwort zu sichern. Richtet die Lehrkraft ein Passwort für die Konferenz ein, ist die Teilnahme an dieser ohne die Eingabe des Passworts nicht möglich.</p>	<p>Der Meeting-Host kann zahlreiche Einstellungen vornehmen, um die Erfüllung dieser Anforderung zu unterstützen:</p> <ul style="list-style-type: none"> Erlaube nur den Zugang authentifizierter Teilnehmer: Der Account-Administrator oder der Meeting-Host können die Teilnahme auf authentifizierte Nutzer (also solche, die in einen Zoom Account eingeloggt sind) beschränken. Dadurch können Personen, die zwar den Meeting-Link, aber nicht eingeloggt sind, nicht am Meeting teilnehmen. Erlaube Zugang nur mit Passcode: Der Account-Administrator oder der Meeting-Host können den Zugang nur nach Eingabe eines Passcodes gewähren. Erzwinge zufallsgenerierten Passcode: Der Account-Administrator kann die Verwendung eines Zufallscodes erzwingen, so dass derselbe Passcode nicht für mehrere Meetings verwendet werden kann. Erlaube Zugang nur von bestimmter Domain: Der Account-Administrator oder der Meeting-Host können den Zugang auf Teilnehmer aus einer bestimmten Web-Domain erlauben - zum Beispiel Nutzer mit einer E-Mail-Adresse einer bestimmten Organisation.

<p>Wartezimmer: Weiterhin sollte das eingesetzte Videokonferenzsystem über einen virtuellen Wartezimmer verfügen. Damit hat die Lehrkraft die Möglichkeit als Moderator den Zugang zur Konferenz zu kontrollieren. In diesem Wartezimmer müssen die Teilnehmer warten, bis die Lehrkraft sie in die eigentliche Konferenz eintreten lässt. Die Lehrkraft erkennt anhand der Namen, wer an der Konferenz teilnehmen möchte. Es sollten also die Klarnamen oder im Vorfeld zur Konferenz abgestimmte Pseudonyme verwendet werden, anhand derer die Lehrkraft erkennen kann, wer sich hinter dem Namen verbirgt.</p>	<p>Der Meeting-Host kann über den Wartezimmer den Zugang zu einer Videokonferenz oder einem Webinar steuern - Teilnehmer können dann vom Host entweder einzeln oder alle auf einmal zum Meeting zugelassen werden.</p> <p>Hier können entweder alle Teilnehmer zunächst in den Wartezimmer geführt werden oder aber eine Ausnahme von der Wartezimmer-Regel für die Teilnehmer aus einer bestimmten Domain eingerichtet werden.</p> <p>Weitere wichtige Funktionalitäten:</p> <ul style="list-style-type: none"> ● Meeting schließen: Es ist darüber hinaus möglich, ein Meeting zu "schließen", so dass keine weiteren Teilnehmer dazu kommen können. ● Verhindere Teilnahme aus bestimmten Ländern / Regionen: Account-Administratoren können die Teilnahme aus bestimmten Ländern oder Regionen über eine "approved vs. blocked list" managen. ● TOR-Blocking: Zoom verhindert die Teilnahme über "The Onion Router (TOR)" und andere IP-Anonymisierungs-Services. <p>Es ist nicht möglich, unerkannt an einem Videokonferenz-Meeting teilzunehmen. Weitere Informationen können im Zoom Help Center gefunden werden.</p>
--	--

3. Sonstige Einstellungen, die die Sicherheit während einer Konferenz erhöhen

Orientierungshilfe	Zoom-Kommentar
Die Lehrkraft ist stets alleiniger Moderator der Konferenz.	Dies ist bei Zoom die Standard-Einstellung. Falls Co-Moderatoren doch einmal erwünscht sind, können diese über die Funktion "Co-Moderator: Dem Host erlauben, Co-Hosts hinzuzufügen" aktiviert werden.
Sie sollte für jede Konferenz einen neuen Einladungs-Link, bzw. neue Meeting-ID sowie ein neues Passwort generieren und den Schülerinnen und Schülern zur Verfügung stellen.	Ja, das ist möglich. Auf der Konto-Ebene (globale Einstellung) kann vorgegeben werden, dass für JEDES spontane sowie geplante Meeting zwingend eine neue Meeting-ID und ein neuer Passcode automatisch generiert werden. Somit ist der Einladungs-Link immer

	<p>eindeutig und nicht wiederverwertbar.</p>
<p>Ein Zutritt zur Konferenz darf ohne die Anwesenheit und Genehmigung der Lehrkraft nicht möglich sein.</p>	<p>Dies ist bei Zoom die Standard-Einstellung.</p> <p>Die Funktion “Teilnehmern Beitritt vor dem Host gestatten” ist daher standardmäßig deaktiviert. Darüber hinaus kann die Option “Wartezimmer” global aktiviert werden. Diese Funktion bewirkt:</p> <p><i>“Wenn Teilnehmer einem Meeting beitreten, setzen Sie sie in einen Wartezimmer und weisen Sie den Host an, sie einzeln einzulassen. Wenn Sie den Wartezimmer freigeben, wird die Einstellung für den Eintritt von Teilnehmern vor dem Host automatisch gesperrt.”</i></p>
<p>Die Lehrkraft muss die Möglichkeit haben, die Konferenz zu schließen, wenn sie beendet ist. Die Konferenz darf nicht weiterlaufen, wenn die Lehrkraft den Raum verlassen hat.</p>	<p>Nur der Moderator hat die Berechtigung, eine laufende Konferenz zu beenden. Sobald der Moderator die Konferenz beendet, werden alle anderen Teilnehmer automatisch getrennt.</p> <p>Darüber hinaus kann eine Funktion aktiviert werden, welche bewirkt, dass Teilnehmer automatisch in den Wartezimmer verschoben werden, wenn der Moderator/ die Lehrkraft das Meeting verlässt oder unerwartet aus der Sitzung gefallen ist (z.B. Verbindungsabbruch). Die Einstellung kann auf Konto-/Gruppen-/Persönlicher Ebene eingestellt werden.</p> <p>Die Einstellung findet man im Zoom Portal unter:</p> <ol style="list-style-type: none"> 1. Admin 2. Einstellungen 3. Meeting 4. Sicherheit 5. Warteroptionsen 6. <i>Verschieben Sie die Teilnehmer in den Wartezimmer, wenn der Host unerwartet aus der Sitzung gefallen ist (muss aktiviert werden)</i>
<p>Es sollte möglich sein, Teilnehmer aus einer Konferenz zu entfernen. Diese Möglichkeit muss alleine bei der Lehrkraft als Moderator liegen.</p>	<p>Ja, bestimmte Teilnehmer können aus laufenden Meetings entfernt werden.</p> <p>Diese Teilnehmer können sich anschließend nicht wieder in das gleiche Meeting einwählen, wenn die Option “Allow removed participants to rejoin” vom Meeting-</p>

	Host nicht aktiviert ist.
<p>Die Möglichkeit, den Bildschirm oder freizugebende Anwendungen (Whiteboards, Präsentationsprogramme) zu teilen, sollte nur der Lehrkraft offenstehen.</p>	<p>Die Zoom-Standardereinstellungen lassen Bildschirmübertragungen (Bildschirm, Inhalte, Whiteboard) aller Teilnehmer zu. Diese Einstellung kann auf Konto-/Gruppen-/Persönlicher Ebene angepasst werden, so dass <u>NUR</u> die Lehrkraft Inhalte teilen darf.</p> <p>Die Einstellung findet man im Zoom Portal unter:</p> <ol style="list-style-type: none"> 1. Admin 2. Einstellungen 3. Meeting 4. In Meeting (Grundlagen) 5. Bildschirmübertragung 6. Wer kann freigeben? Hier muss “Nur Host” ausgewählt werden 7. Zoom empfiehlt hierzu noch die folgende Einstellung zu aktivieren. <ol style="list-style-type: none"> a. Annotation b. Standardmäßig kann nur der Benutzer, der den Bildschirm freigibt, Anmerkungen machen
<p>Das Chatten zwischen den Teilnehmern sollte unterbunden werden.</p>	<p>Hierzu muss entweder die Einstellung “Chat” oder “Privater Chat” deaktiviert werden. Diese Einstellung(en) kann auf Konto-/Gruppen-/Persönlicher Ebene deaktiviert werden.</p> <p>Die Einstellungen findet man im Zoom Portal unter:</p> <p><u>Chat</u></p> <ol style="list-style-type: none"> 1. Admin 2. Einstellungen 3. Meeting 4. Besprechung planen 5. Chat (deaktivieren) <ol style="list-style-type: none"> a. bewirkt, dass die Chat-Funktion komplett deaktiviert wird <p>Privater Chat</p> <ol style="list-style-type: none"> 1. Admin

	<ol style="list-style-type: none"> 2. Einstellungen 3. Meeting 4. Besprechung planen 5. Privater Chat (deaktivieren) <ol style="list-style-type: none"> a. bewirkt, dass Teilnehmer untereinander keine privaten Nachrichten mehr senden können b. Chat mit der Lehrkraft ist weiterhin möglich
<p>Die Lehrkraft sollte die Möglichkeit haben, einzelne Kameras und Mikrofone abzuschalten.</p>	<p>Moderatoren haben generell die Möglichkeit, die Kamera oder das Mikrofon eines Teilnehmers zu deaktivieren.</p>