

Jennifer Eickelmann; Sophie G. Einwächter; Felix T. Gregor; Ulrike Hanstein;
Sandra Kero; Elisa Linseisen

Handreichung zur Gewaltprävention in Lehr- und Lernkontexten online

2021

<https://doi.org/10.25969/mediarep/15780>

Veröffentlichungsversion / published version

Buch / book

Empfohlene Zitierung / Suggested Citation:

Eickelmann, Jennifer; Einwächter, Sophie G.; Gregor, Felix T.; Hanstein, Ulrike; Kero, Sandra; Linseisen, Elisa: *Handreichung zur Gewaltprävention in Lehr- und Lernkontexten online*. 2021. DOI: <https://doi.org/10.25969/mediarep/15780>.

Nutzungsbedingungen:

Dieser Text wird unter einer Creative Commons - Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 Lizenz zur Verfügung gestellt. Nähere Auskünfte zu dieser Lizenz finden Sie hier:

<https://creativecommons.org/licenses/by-sa/4.0>

Terms of use:

This document is made available under a creative commons - Attribution - Share Alike 4.0 License. For more information see:

<https://creativecommons.org/licenses/by-sa/4.0>

Handreichung zur Gewaltprävention in Lehr- und Lernkontexten online

(Stand 17.04.2021)

Jennifer Eickelmann, Sophie G. Einwächter, Felix T. Gregor, Ulrike Hanstein, Sandra Kero, Elisa Linseisen

Einleitung

1. Hinweise für die Vorbereitung von digitalen (Lehr-)Veranstaltungen

1.1 Auseinandersetzung mit Veranstaltungstyp, -inhalten und antizipiertem Publikum

1.2 Auseinandersetzung mit Software/Plattformen

1.3 Konkrete Planung

1.3.1 Rechtsgrundlagen

1.3.2 Zugang und Einlasskontrolle

1.3.3 Informationen und Vereinbarungen zur Netiquette und Antidiskriminierung

1.3.4 Antidiskriminierung in der Lehre

2. Umgang mit gewaltförmigen Störungen

2.1 Diskussionsstörungen und Wortergreifungsstrategien

2.2 Zoombombing oder andere Störungen von Meetings (Bild, Text und Ton)

2.3 Rechtlicher Schutz, Meldestellen und Rechtsberatung

Quellen

Einleitung

Die Covid-19-Pandemie hat das wissenschaftliche Lehren und Lernen grundlegend verändert und weitestgehend auf digitale Medien ausweichen lassen. Eine Begleiterscheinung ist, dass die mit der Digitalisierung einhergehenden neuen Sichtbarkeiten sowie Öffnungen von Interaktionsräumen neue Verletzlichkeiten schaffen, welche von verschiedenen Akteur*innen mit unterschiedlicher Motivation ausgenutzt werden können. So gibt es zum einen eine Zunahme von als zielgerichtet anzunehmenden, politisch motivierten, Angriffen (etwa gegen Frauen* online, gegen Angehörige von ethnischen Minderheiten, Vertreter*innen der Gender Studies, gegen Personen, die sich offen antirassistisch positionieren, und generell gegen Veranstaltungen diversitätsorientierter Forschung und Lehre) (vgl. Evans 2019). Weltweit ist eine Zunahme von wissenschaftsfeindlichen Positionen zu beobachten, die ebenfalls mit politischem Kalkül und zunehmender Vehemenz vertreten werden. Zum anderen ist in digitalen Umgebungen aber auch von Angriffen und Störungen auszugehen, die vorgenommen werden, einfach, *weil sie möglich sind* und Täter*innen (vermeintlich) anonym und so oftmals ungestraft agieren können (vgl. Meineck und Schwenn 2020). Um Prävention zu betreiben, gilt es deshalb, die medientechnologischen Bedingungen in den Blick zu nehmen, die ihnen Angriffsflächen bieten können.

Ein anonym auf den geteilten Bildschirm gekritzelt Hakenkreuz, unerwünschte sexuell konnotierte Kontaktaufnahmen über den privaten Chat am Rande einer wissenschaftlichen Veranstaltung, die koordinierte Stürmung eines Zoom-Vortrags durch störende Unbekannte... In den letzten Monaten waren auch in der Medienwissenschaft erste übergriffige Vorfälle und ‚Zoombombing‘¹ bei Vortragsveranstaltungen online zu beobachten, die Abläufe massiv störten. Ebenso gibt es in der digitalisierten Lehre Situationen, die missachtende oder diskriminierende Effekte zeitigen können und die bislang vielerorts noch nicht ausreichend reflektiert werden.

¹ Externe Personen betreten, teils koordiniert und zumeist anonym, das Meeting und stören dieses auf sicht- und hörbare Weise massiv. Über geteilte Bildschirme oder Kamerafunktion teilen oder zeigen sie pornografische, gewalttätige, rassistische, antisemitische oder frauenfeindliche Bilder, Gesten oder Schriftinhalte (vgl. Gleichstellungsbüro der RUB und Zentrum Wissenschaftsdidaktik 2021: 2).

Die vorliegende Handreichung wurde von Medienwissenschaftler*innen, orientiert an einem organisatorischen beziehungsweise pragmatischen Bedarf im eigenen Fach zusammengestellt. Ihr Ziel ist, dafür zu sensibilisieren, dass digitalisierte, virtuelle Umwelten und Sichtbarkeiten Gefährdungspotenziale bergen, die insbesondere in der Lehre und bei der Planung von Online-Veranstaltungen mitgedacht werden sollten. Während uns also daran liegt, einen Diskurs innerhalb der Medienwissenschaft anzuregen, sind Vorhaben und Leitfäden doch anschlussfähig für Lehrende anderer Disziplinen.

Insbesondere aufgrund dieser Anschlussfähigkeit ist uns wichtig zu betonen, dass die vorgeschlagenen Handlungsoptionen jeweils kontextabhängig sind und nicht für jede Veranstaltung oder jeden Personenkreis optimal sein müssen. Auch bergen die verwendeten Softwares ggf. eigene Besonderheiten oder Angriffsmöglichkeiten, zu denen es spezifische Lösungswege gibt. Wir verweisen an geeigneter Stelle auf ausführlichere Erklärungen und bereits veröffentlichte Leitfäden, um diese Handreichung knapp zu halten und zugleich die Möglichkeit zur Vertiefung zu geben.

Die vorliegende Fassung versteht sich – technologisch bedingt – als eine Momentaufnahme und als Work-In-Progress: Wir freuen uns über Ergänzungen und Hinweise auf Auslassungen oder Unstimmigkeiten an die institutionellen Email-Adressen der Autor*innen. Bei Bedarf wird eine erweiterte Version erstellt, die diesen Rückmeldungen Rechnung trägt.

Für die wissenschaftliche Praxis empfehlen wir besonders nachfolgende Situationen daraufhin zu reflektieren, inwiefern sie Angriffsflächen für Störungen und Formen von Missachtungen, Diskriminierungen und Gewalt bieten:

- **Öffentliche Veranstaltungen online** (z.B. Tagungen, Vorlesungen, Diskussionsformate)
- **Lehrveranstaltungen online** (im Plenum, aber auch Breakout-Rooms, private Chats innerhalb des offiziellen Lehr- und Lernsettings)

Digitale Missachtungen und Gewalt können psychische, physische sowie gesellschaftliche Folgen haben und sich auch in anderen Räumen fortsetzen. Angriffe und Bedrohungen im Digitalen sind in keiner Weise harmlos oder ‚nicht real‘. Hierbei gilt es nicht nur die Perspektive der Lehrenden einzunehmen, sondern auch jene der Studierenden mitzudenken. Denn einen risikobewussten Umgang mit Verletzlichkeiten in Lehr- und Lernkontexten zu thematisieren und zu schulen, kommt qua Diskussion und Vorbild auch der studentischen Praxis zugute.

1. Hinweise für die Vorbereitung von digitalen (Lehr-)Veranstaltungen

1.1 Auseinandersetzung mit Veranstaltungstyp, -inhalten und antizipiertem Publikum

Es wird empfohlen, sich im Vorfeld einer Veranstaltung zu vergegenwärtigen, was thematischer **Schwerpunkt und Zielsetzung** sowie Zielgruppe und anzunehmende Teilnehmer*innenzahl der Veranstaltung sind (vgl. LHM und MBR 2014: 15). Auch sollte geklärt werden, ob es sich um eine für die Öffentlichkeit **zugängliche oder geschlossene** Veranstaltung handeln soll und welche Form der Interaktion mit den Teilnehmenden (etwa: moderierte Diskussion, Chat o.ä.) angeboten werden soll (ebd.). Aus diesen Entscheidungen ergeben sich in Abstimmung mit der institutionellen Infrastruktur, vorhandenen Lizenzen und Supportangeboten am jeweiligen Standort die Wahl der Software sowie benötigte personelle Ressourcen.

Wann immer eine Beteiligung der Öffentlichkeit oder ein nicht überschaubarer Personenkreis anzunehmen sind, sowie bei kontroversen Inhalten und Themen, bietet sich eine mindestens

doppelte Moderation und Administration an (z.B. eine technisch orientierte Instanz, die Personen zulässt oder ggf. sperrt, und eine inhaltlich ausgerichtete). Idealerweise kann auch für die Moderation des Chats eine Person bereitgestellt werden, die sich ausschließlich dieser Aufgabe widmen kann. Ein großes Team kann so **Überforderungssituationen abwenden**. Im Umkehrschluss heißt das auch: Wenn nur eine Person allein die Sitzung moderieren und administrieren kann, sollte überdacht werden, ob ein paralleler Chat noch sinnvoll eingebunden werden kann. Im Seminargeschehen ließe sich diese Aufgabe hingegen auch an Freiwillige delegieren.

In jedem Fall sollte vorab erwogen werden, welche Sichtbarkeiten durch die Veranstaltung geschaffen werden, und ob diese dem Veranstaltungszweck dienlich sind: Verlangt das Geschehen eine **Sichtbarkeit (mit eingeschalteter Kamera)** vonseiten aller Teilnehmenden oder nur von einzelnen Hauptakteur*innen?

Während die Sichtbarkeit per Kamera sowie mittels der **Verwendung von Klarnamen** Transparenz und Verbindlichkeit im Seminargeschehen fördern kann, bedeutet gekoppelte Bild/Klarnamen-Information (ggf. noch gesteigert durch **Einblicke in private Innenräume, familiäre Situationen** o.ä.) auch eine gesteigerte Verletzlichkeit, die eine Interaktion hemmen kann und – sofern sie eingefordert wird – auch als machtvoller Übergriff aufgefasst werden kann. Darüber hinaus sollte die Notwendigkeit einer Teilnahme mit eingeschalteter Kamera auch aus Gründen der **Datensparsamkeit und Sitzungsstabilität** sowie aus **Nachhaltigkeitsgründen** hinterfragt werden. So fällt der CO²-Verbrauch einer Veranstaltung mit ausgeschalteter Kamera um ein Vielfaches geringer aus (vgl. Gröger 2020).

1.2 Auseinandersetzung mit Software/Plattformen

Wir empfehlen vor dem Einsatz in einer Veranstaltung eine ausführliche Auseinandersetzung mit der Plattform und/oder Software, die genutzt werden soll. **Firmeneigene FAQs und Help Center** informieren über spezifische Eigenschaften, Voreinstellungen und Befugnisse für Hosts von Veranstaltungen:

[Zoom](#), [BigBlueButton](#), [Cisco WebEx](#), [Microsoft Teams](#), [Miro Board](#), [Go To Meeting](#).

Viele Hochschulen bieten zudem Beratungen in Bezug auf die eingesetzten Tools an, so dass bei Unsicherheiten eine Rücksprache mit den entsprechenden IT-Zentren empfohlen wird.

In den Grundeinstellungen zum Bereich „Sicherheit“ können einige unerwünschte/ missbrauchsanfällige Interaktionsmöglichkeiten und Funktionen von vornherein ausgeschaltet werden (wie etwa das **Annotieren oder Kommentieren von Bildinhalten**, welche oft von Störer*innen genutzt werden, indem auf geteilte Bildschirme geschrieben wird). Auch die **Funktion des Bildschirmteilens** sollte nur bei Bedarf von der Meeting-Leitung für einzelne andere Personen freigegeben werden. Wird die Funktion allgemein für alle Teilnehmer*innen freigegeben, kann dies auch missbräuchlich genutzt werden. Bei großen Meetings bietet sich deshalb an, gezielt diejenigen Personen zu Hosts zu machen, welche Material teilen sollen, um weiterhin Freigaben begrenzt zu halten.

1.3 Konkrete Planung

1.3.1 Rechtsgrundlagen

In Online-Veranstaltungen gelten **Urheberrecht, Persönlichkeitsrecht wie auch das Strafrecht** gleichermaßen wie offline. Die Rechtsabteilungen und IT-Zentren der Universitäten stellen für rechtliche Fragen der digitalen Veranstaltungsorganisation Ansprechpartner*innen oder online verfügbare Hinweise bereit.

Es empfiehlt sich, zu Beginn der Veranstaltung oder vorab, etwa bei Anmeldung, darauf hinzuweisen, dass vom **virtuellen Hausrecht** Gebrauch gemacht wird, d.h. Störungen der Veranstaltung (je nach Umfang) mit Abschalten von Kamera/Ton der störenden Person und bei entsprechender Schwere auch mit einem Ausschluss der Person aus der Sitzung geahndet werden bzw. bei Straftatbestand auch Anzeige erstattet wird.

Wenn Teile der Veranstaltung aufgezeichnet werden sollen, muss eine **schriftliche Erlaubnis der aufzuzeichnenden Personen** vorliegen.² Andere Teilnehmende sollten in diesem Fall eigene Mikrophone und Videos ausschalten um die Aufzeichnung nicht zu stören und um ihre Privatsphäre zu schützen. **Aber Vorsicht:** Manche Softwares (z.B. BigBlueButton, siehe [hier](#)) zeichnen Sitzungen auch ohne Aufzeichnungsbefehl automatisch auf, wenn die Aufnahme-funktion nicht vorab deaktiviert wurde.

1.3.2 Zugang und Einlasskontrolle

Zur Vermeidung unbekannter Störer*innen empfiehlt sich eine namentliche Anmeldung vorab sowie die Herausgabe von **Sitzungslink und Passwort nur an Angemeldete, mit der Bitte um Vertraulichkeit**.

Das Verwenden eines Warteraums, wie er in den meisten Softwares voreingestellt ist, wird empfohlen. Hier können Wartende anhand der Anmeldungsliste überprüft und ggf. einzeln zugelassen werden. Erscheint hier ein unbekannter Name, so kann die Person bei den meisten Softwares bereits innerhalb des Warteraums angeschrieben und um Aufklärung oder Anpassung des eigenen Namens gebeten werden. **Vom offenen Posten von Links zu Veranstaltungen**, bei denen Teilnehmende selber hörbar und sichtbar sein können oder Bildschirme teilen bzw. kommentieren können, **wird ausdrücklich abgeraten**. So gibt es Gruppen, die sich online nur zum Zwecke der Veranstaltungsstörung vernetzen – einmal entdeckte Links werden hier schnell geteilt und Attacks koordiniert (vgl. Meineck und Schwenn 2020). Bei einigen Softwareanbietenden sind zusätzliche Funktionen zur Authentifizierung vorgesehen, wie etwa eine Vorab-Anmeldung über die Software selbst. Finden Veranstaltungen im großen Kreis wiederholt bzw. in Serie statt, empfiehlt sich das **Generieren neuer Links für jedes Meeting**, um unerwünschte Weitergaben von Anmeldeinformationen gering zu halten.

Allerdings gilt: Aufwand und Nutzen von Anmeldungsmodalitäten sind immer abzuwägen. Eine kleine, einander bekannte Gruppe mag intern gefahrlos durchaus auch die gleichen Meeting-Kenndaten wiederholt verwenden. Verbindliche Anmeldungen und vorab formulierter Einlassvorbehalt sollten aber genutzt werden, wenn eine Störung als wahrscheinlich gilt oder der Personenkreis nicht überschaubar ist (vgl. LHM und MBR 2014: 14). Wenn die antizipierte Gruppe vollständig ist, bietet die verwendete Plattform ggf. die **Möglichkeit, den Raum zu schließen**, damit keine weiteren Personen eintreten können (z.B. bei Zoom über Sicherheit → Meeting Sperren).

1.3.3 Informationen und Vereinbarungen zur Netiquette und Antidiskriminierung

Die meisten Universitäten (bzw. ihre Antidiskriminierungs- oder Gleichstellungsbeauftragten) stellen bereits eigene **Leitlinien zur Netiquette** und zum **diskriminierungsfreien Umgang** in der digitalen Lehre bereit (vgl. etwa Uni Göttingen/Stabstelle Chancengleichheit 2020, Gleichstellungsbüro der RUB & Zentrum Wissenschaftsdidaktik 2021, Antidiskriminierungsstelle für

² Eine detaillierte [Anleitung zur Einholung des Einverständnisses](#) mit Handlungsempfehlungen gibt es online, bereitgestellt vom Team digitales Lernen und Lehren der Georg-August-Universität Göttingen („Persönlichkeitsrecht Bild- /Tonaufnahmen“ 2020).

Studierende der Uni Marburg 2020 uvm.). Diese können sowohl zur Vorbereitung der Teilnehmenden als auch als konkrete **Richtlinien und Teilnahmekonsens** für universitäre Veranstaltungen genutzt werden. Über den Umgang mit diesen Leitlinien lernen Studierende auch bereits die Anlaufstellen kennen, die sie im Fall von erlebten Diskriminierungen kontaktieren können.

Bei Ankündigungen von Konferenzen und Workshops können Veranstalter*innen auf die erwähnten Dokumente verlinken oder eigene **Prinzipien zum Umgang mit Diskriminierung und Belästigung** erklären und zur Anmeldevoraussetzung machen. Teilnehmende können hier aufgefordert werden, nur dann der Sitzung beizutreten, wenn sie sich bereiterklären, von Aufzeichnungen, Störungen, Beleidigungen oder Verstößen gegen Persönlichkeits- und Urheberrechte abzusehen. Die jeweilige Umsetzung hängt vom Setting ab: Manche Softwares erlauben die Einblendung einer individuellen Start-Information, die akzeptiert werden muss, um beizutreten (wie etwa „customized disclaimers“ in Zoom); in E-Learning-Umgebungen wie Moodle kann die Beantwortung einer Frage (z.B. „Haben Sie die Kursregeln gelesen und stimmen diesen zu?“) in Form eines Tests zur Voraussetzung für die Kursteilnahme gemacht werden. Die transparente Kommunikation und gemeinsame Vereinbarung von Regeln vorab erleichtern ein Handeln im Ernstfall der Störung und vermitteln, dass der Sitzungsleitung am Schutz der Teilnehmenden gelegen ist.

1.3.4 Antidiskriminierung in der Lehre

Wichtigster Schwerpunkt der Antidiskriminierung innerhalb der digitalen Lehre ist die Schaffung eines Angebots, das möglichst für alle Studierende auch in der Krisensituation der Covid-19-Pandemie wahrnehmbar sein soll. Einen wichtigen Aspekt stellt hier die generelle **Flexibilisierung der Teilnahmeoptionen** dar (vgl. Gleichstellungsbüro der RUB und Zentrum Wissenschaftsdidaktik 2021: 1; Heinke et al. 2020). Findet Lehre ausschließlich innerhalb von verpflichtenden Live-Veranstaltungen in Videokonferenzen statt, kann dies Personen ausschließen, die Betreuungsaufgaben nachgehen müssen oder nicht die technischen Mittel besitzen, eine störungsfreie Verbindung aufrechtzuerhalten (ebd.). Ein **Wechsel von asynchronen und synchronen Formaten** oder die Bereitstellung der wichtigsten Inhalte in asynchroner Form kann hier Abhilfe schaffen.

Um einen vertrauensvollen Raum für digitale Interaktion zu schaffen, sollte auch in der Lehre eingangs geklärt werden, dass von **Screenshots oder Aufzeichnungen** abgesehen werden soll, und welche Regeln innerhalb des Kurses und innerhalb der Gruppenarbeitsräume eingehalten werden sollen. Um Konzentration zu gewährleisten und unerwünschte Kontaktaufnahmen innerhalb des Kurses untereinander zu umgehen, kann die Funktion des **persönlichen Chats vorab ausgestellt** werden. Allerdings empfiehlt sich, in Erfahrung zu bringen, ob der private **Chat mit der Kursleitung** weiterhin möglich ist (wie etwa bei Zoom). Dies kann ein wichtiger Kanal für Studierende sein, mitzuteilen, was sie nicht vor dem gesamten Kurs besprechen möchten (z.B. Grund für ausgeschaltete Kamera, früheres Verlassen der Sitzung oder bevorzugt stille Teilnahme). Ebenfalls kann abgesprochen werden, das Meeting immer etwas früher zu beginnen und/oder Studierende selbständig nach dem Ende austreten zu lassen, damit Personen mit Rückfragen oder individuellen Anliegen diese noch vorbringen können.

Studierende sollten für die Lehrperson **identifizierbar** sein, aber nach Möglichkeit **nicht zu Klarnamen oder Kameraverwendung gezwungen werden** (vgl. Gleichstellungsbüro der RUB und Zentrum Wissenschaftsdidaktik 2021: 3). Studierende können etwa im Vorfeld der ersten Sitzung gebeten werden, sich bei der Kursleitung zu melden, wenn sie lieber mit einem

Aliasnamen oder einem anderen als im System geführten Namen im Kurs angesprochen werden möchten. Dies kann auch von Relevanz sein, wenn Studierende keine Übertragung ihrer persönlichen Daten an einen kommerziellen Dienstleister wie Zoom wünschen (vgl. Uni Göttingen, „Nutzung von Zoom“, 2020: 3). Um **falsche Ansprachen** zu vermeiden, sollten Studierende darüber hinaus auf die Option hingewiesen werden, neben ihre Namen in Klammern ihre **bevorzugten Pronomen** aufzuschreiben (vgl. Gleichstellungsbüro der RUB und Zentrum Wissenschaftsdidaktik 2021: 3).

Die **Privatsphäre der Studierenden** verdient Schutz. Weisen Sie sie darauf hin, dass sie Bildhintergründe unkenntlich machen können oder Kameras ausgeschaltet lassen können. Auch bei der Nutzung von Abstimmungstools oder der Bezugnahme auf eingereichte Aufgaben von Studierenden sollte nach Möglichkeit auf Anonymität geachtet werden, um Stress oder Bloßstellung zu vermeiden (vgl. u.a. Bittner und Garske 2020).

2 Umgang mit gewaltförmigen Störungen

2.1 Diskussionsstörungen und Wortergreifungsstrategien

Innerhalb von Diskussionsformaten und in Seminarkontexten kann es insbesondere im Kontext von politischen Themen wie Klimawandel, aktuelle Migrationspolitik, Reflexion von Kolonialismus sowie Feminismus und Gleichstellungsfragen zu gezielten **Wortergreifungen politisch motivierter Akteur*innen** kommen, die eine sachliche Diskussion unterlaufen oder den Gegenstand der Diskussion grundlegend infrage stellen – und somit auch eine beabsichtigte Störung darstellen. In einer Handreichung der Stadt München, die mit der Mobilen Beratung gegen Rechtsextremismus Berlin erstellt wurde, wird gefolgert: „Im schlimmsten Fall werden Veranstalter[*innen] durch schlechte Erfahrungen (aus dem Ruder gelaufene oder ‚gekaperte‘ Diskussionen, rechtliches Nachspiel oder beleidigende Hassmails) davon abgehalten, sich bestimmten Themen zu widmen und bestimmte Veranstaltungen durchzuführen“ (LHM und MBR 2014: 9).

Zur Auseinandersetzung mit solchen oft formelhaften Gesprächsmustern empfehlen wir an dieser Stelle Leitfäden, die sich mit diesen **Wortergreifungsstrategien der extremen Rechten** auseinandersetzen und Vorschläge unterbreiten, wie **demokratische Debattenkultur und die Sachebene** auch innerhalb kontroverser Diskussionen gewahrt werden können (hier stellvertretend und weiterführend: MBR und VDK Berlin 2010; Rosa Luxemburg Stiftung 2017). Das Fortbildungsteam Gegen-Argument (www.gegen-argument.de) plädiert dafür, je nach Inhalten der vorgebrachten Wortergreifung und der eigenen Verfasstheit argumentativ vorzugehen, sich zu positionieren und damit ein Signal der Nichtzustimmung zu setzen oder – im Falle **strafrechtlicher Relevanz oder starker Herabwürdigung von Menschen** – die betreffenden Teilnehmenden stumm zu schalten und ggf. offline Kontakt zu suchen (interne Webinar-Folien „Umgang mit (extrem) rechten Störungen in der digitalen Lehre“, 2020). Wichtig ist – insbesondere im Seminarzusammenhang – die Verantwortung der Kursleitung für die Gruppe der Teilnehmer*innen, die es zu schützen gilt. Eine **Nachbesprechung von Vorfällen** ist in jedem Fall angebracht.

2.2 Zoombombing oder andere Störungen von Meetings (Bild, Text und Ton)

Passiert eine Störung oder eine Form des Angriffs, handelt es sich meist um eine überraschende Situation, in der möglichst zügige Schadensbegrenzung betrieben werden sollte. Unerlaubt gezeigte Videoinhalte von Störer*innen können **traumatisierenden Charakter** haben (vgl.

Someone might try to...	BEFORE your meeting you can...	In addition to removing someone (above), DURING your meeting you can...
Join your online meeting/training uninvited or too early	<ul style="list-style-type: none"> • Require a password to join your meeting (now enabled by default) • Change your meeting ID for each session • Not post log-in information for your sessions publicly like in social media • Customize your waiting room message to include guidelines for participation 	<ul style="list-style-type: none"> • Enable waiting room from the toolbar Security menu • Only approve people to enter the room (using the Participants menu) those who you are expecting • Lock your meeting after the right people are in the room using the Security menu in your toolbar
Say disruptive things out loud		<ul style="list-style-type: none"> • Mute them by clicking on the menu next to their name in the Participants menu • Prevent people from unmuting themselves: In the More menu at the bottom of the Participants menu, check Mute participants upon arrival and uncheck Allow Participants to Unmute themselves
Say disruptive things publicly in chat	<ul style="list-style-type: none"> • Disable Chat for all meetings in the Zoom account settings under In Meeting (Basic) - <i>Not recommended because it limits engagement and accessibility.</i> 	<ul style="list-style-type: none"> • Change the chat settings: In the chat box, click the ... button and change to Participant Can Chat with: Everyone publicly or Host only or No one • Disable chat: From the Security menu in your toolbar, uncheck Chat under Allow Participants to...
Say disruptive things to people using private chat	<ul style="list-style-type: none"> • Turn off Private chat for all meetings in the account settings under In Meeting (Basic) - <i>Not recommended because it limits participants' ability to communicate confidentially with the hosts.</i> 	<ul style="list-style-type: none"> • Change the chat settings: In the chat box, click the ... button and change to Participant Can Chat with: Everyone publicly or Host only or No one • Invite participants to let you know if they are getting disruptive private chats
Share files in the chat box that are disruptive	<ul style="list-style-type: none"> • Turn off file sharing for all meetings: Turn off chat file sharing in your Zoom account settings. Find this in File transfer under In Meeting (Basic) 	
Show something disruptive on their web camera	<ul style="list-style-type: none"> • Turn off virtual background in your Zoom account settings under In Meeting (Advanced) 	<ul style="list-style-type: none"> • Turn off their web camera: From the participants menu or on their camera on gallery/speaker view, click ... or More and choose Stop video
Show something disruptive using screen sharing	<ul style="list-style-type: none"> • Disable Participant Screen Sharing for all meetings: Set your Account settings so that only hosts can share screen under In Meeting (Basic)- <i>Not recommended if you regularly hold meetings where various people share screens.</i> 	<ul style="list-style-type: none"> • Stop screen share. • Disable participant screen sharing: From the Security menu in your toolbar, uncheck Share Screen under Allow Participants to...
Write/draw something disruptive on screen share using the Annotate feature	<ul style="list-style-type: none"> • Disable Attendee Annotation for all meetings: Turn Annotation off in your Zoom account settings under In Meeting (Basic). 	<ul style="list-style-type: none"> • Disable Attendee Annotation: After starting a screenshare, from the toolbar Security menu, uncheck Annotate Shared Content under Allow Participants to... • Clear the annotation by clicking Annotate in your main toolbar, then click Clear

Abb.1: Sicherheit in Zoom (aus Rewa 2020: 4-5)

bar informiert werden, je nach Art des Vorfalls (z.B. rassistisch, antifeministisch motiviert) auch die Gleichstellungsbüros/Antidiskriminierungsstellen. Betroffene, aber auch Personen, die von

Meineck und Schwenn 2020) und müssen schnellstmöglich unterbunden werden.

Das Dokument „Dealing with disruptors in Zoom online meetings or trainings“ von Jeanne Rewa (2020) listet konkrete Handlungsmöglichkeiten je nach Art der Störung auf (vgl. Abb.1).

Ist bei einer massiven Störung erkennbar, von wem diese ausgeht, sollte diese Person direkt aus dem Meeting entfernt werden. Ist unklar, ob es sich um mehrere Störende handelt, sollte das **Meeting ganz beendet oder pausiert** werden (z.B. in Zoom über Sicherheit → alle Aktivitäten der Teilnehmer beenden), indem die **Sitzung vorübergehend gesperrt** wird, was auch neue Zutritte in dieser Zeit verhindert (vgl. Gleichstellungsbüro der RUB und Zentrum Wissenschaftsdidaktik 2021: 4).

Die Veranstalter*innen müssen reagieren, wenn Diffamierungen oder andere strafrechtlich relevante Störungen stattgefunden haben, etwa wenn verfassungsfeindliche Symbole, pornografische und/oder Gewaltbilder oder -videos verbreitet wurden: „Sind während der Veranstaltung [...] **Straftaten** begangen worden, sollte die Polizei informiert werden [...]. Bei manchen Straftatbeständen [...] (z.B.) Verstoß gegen das Recht am eigenen Bild) ist auch die Stellung eines Strafantrags durch den Verletzten erforderlich. Nähere Informationen hierzu erhält man bei jeder örtlichen Polizeidienststelle“ (LHM und MBR 2014: 20).

Bei Vorfällen in Lehrveranstaltungen oder öffentlichen akademischen Veranstaltungen sollten die IT-Abteilungen und die Justiziarate der Hochschule unmittel-

den Vorfällen Kenntnis haben, können Beschwerdestellen der Hochschulen ansprechen, um eine **Aufarbeitung der Vorfälle** und ggf. **Sanktionen gegen Täter*innen** zu bewirken.

Vorfälle sollten umfassend dokumentiert werden: Art des Vorfalls, Datum und Uhrzeit, beteiligte Personen, geschädigte Personen. Bei Hasskommentaren sollten Screenshots den Kommentartext, Datum, Uhrzeit und den Nutzer*innennamen der*des mutmaßlichen Täters*in zeigen. Die **Dokumentation** sollte deutlich machen, gegen wen sich der Kommentar richtet.

Auch bei Zoombombings können Screenshots vom Tatbestand und Täter*innen angefertigt werden, die **Dokumentation des Ereignisses sollte aber nicht zu einer Verlängerung der strafbaren Situation** führen; es ist davon auszugehen, dass genug potenzielle Zeug*innen anwesend sind/waren, die hinterher über den Vorfall Auskunft geben können. Die Störung kann auch über ein Gedächtnisprotokoll dokumentiert werden.

Die genannten Störungen stellen in aller Regel auch **Verstöße gegen die Richtlinien der Software-Anbietenden** dar und sollten diesen ebenfalls gemeldet werden, damit diese ggf. ihre Sicherheitsvorkehrungen optimieren.

2.3 Rechtlicher Schutz, Meldestellen und Rechtsberatung

Ein ab dem 3. April 2021 in Kraft getretenes Gesetzespaket gegen Hass und Hetze (BMJV 2021) verschärft die **Sanktionierung von Hass online**, indem das Strafmaß für Bedrohungen und Beleidigungen im Netz erhöht wird. Außerdem werden die Betreibenden von Social Media-Plattformen stärker in die Pflicht genommen: „Ab Februar 2022 müssen soziale Netzwerke Mord- und Vergewaltigungsdrohungen und andere schwere Hassdelikte nicht mehr nur löschen, sondern auch dem Bundeskriminalamt melden“ (BMJV 2021).

Das ist auch deshalb von Bedeutung, weil Wissenschaftler*innen auch abseits der oben genannten Lehr- und Lernsituationen Opfer digitaler Gewalt werden können, nämlich über **Email oder Messengerdienste**, generell über **Individualprofile und Kanäle in Social Media oder auf öffentlichen Webseiten**, insbesondere bei der Verwendung von Klarnamen und personenbezogener geteilter Information. Auch diese Orte der digitalen Interaktion, die nicht Schwerpunkt der vorliegenden Handreichung waren, sollten daraufhin reflektiert werden, welche Sichtbarkeiten sie schaffen und welche Verletzlichkeiten damit einhergehen könnten.

Wir schließen unsere Handreichung mit **Anlaufstellen und Unterstützungsangeboten** für Opfer digitaler Gewalt:

Eine wichtige **außeruniversitäre Meldestelle** von Hassrede, Beleidigung, Bedrohung oder anderer digitaler Gewalt ist die **Polizei**. Strafanzeigen werden bei örtlichen Polizeidienststellen sowie online aufgenommen, über: <https://online-strafanzeige.de>.

Es gibt überdies **gemeinnützige Initiativen**, die gemeldete Vorfälle juristisch prüfen, Betroffene individuell beraten und unterstützen und gegebenenfalls Vorfälle auch stellvertretend zur Anzeige bringen:

- Hassmelden – Zentrale Meldestelle für *Hate Speech*: <https://hassmelden.de/>
- *HateAid* – Beratungsstelle für Betroffene von digitaler Gewalt: <https://hateaid.org/>
HateAid bietet individuelle Rechtsberatung an und unterstützt bei der Rechtsdurchsetzung, der Prozesskostenfinanzierung sowie dem Löschen von Inhalten.
- RIAS – Recherche- und Informationsstelle Antisemitismus: <https://report-antisemitism.de/>
RIAS dokumentiert antisemitische Vorfälle und unterstützt Betroffene psychosozial und juristisch.

Trotz des Schwerpunkts dieser Handreichung stehen für uns die konstruktiven Aspekte des Austauschs und der Zusammenarbeit, die durch digitale Interaktionsformate möglich werden, klar im Vordergrund! In diesem Sinne wünschen wir allen Leser*innen gelungene Online-Veranstaltungen und viele positive Erfahrungen mit der Online-Lehre!³

Quellen

- Antidiskriminierungsstelle für Studierende der Uni Marburg (2020): Antidiskriminierung und Persönlichkeitsrechte in der digitalen Lehre. www.uni-marburg.de Juli 2020. Online: https://www.uni-marburg.de/de/universitaet/administration/verwaltung/stabsstellen/adis/diskriminierungsschutz-und-digitale-lehre_0720.pdf
- Bittner, Melanie und Pia Garske (2020): Gender-/Diversitätsreflexivität in der digitalen Lehre: Respektvolle Kommunikation fördern – Übergriffe vermeiden – schwierige Situationen bewältigen. www.hochschulforumdigitalisierung.de 26. Oktober 2020. Online: <https://hochschulforumdigitalisierung.de/de/blog/respektvolle-kommunikation-online-lehre>
- BMJV (Bundesministerium der Justiz und für Verbraucherschutz) (2021). „Gesetzespaket gegen Hass und Hetze tritt am 3. April 2021 in Kraft“. www.bmjbv.de 1. April 2021. Online: https://www.BMJV.de/SharedDocs/Artikel/DE/2021/0401_Gesetzespaket_gegen_Hass_und_Hetze.html.
- Evans, Jennifer (2019): Der neue Kampf gegen die Gender Studies. www.geschichtedergewenwart.ch, 6. März 2019. Online: <https://geschichtedergewenwart.ch/der-neue-kampf-gegen-die-gender-studies/print/>
- Gröger, Jens (2020): Digitaler CO2-Fußabdruck – Datensammlung zur Abschätzung von Herstellungsaufwand, Energieverbrauch und Nutzung digitaler Endgeräte und Dienste. Im Auftrag des Bund für Umwelt und Naturschutz Deutschland e.V. (BUND). www.oeko.de, 14. Juli 2020. Online: <https://www.oeko.de/fileadmin/oekodoc/Digitaler-CO2-Fussabdruck.pdf>
- Meineck, Sebastian und Paul Schwenn (2020): VICE-Recherche: So attackieren Zoom-Bomber private Videokonferenzen mit Kinderpornografie. www.Vice.com 3. Juni 2020. Online: <https://www.vice.com/de/article/m7ie5y/zoom-bombing-unsichere-zoom-meetings-von-trollen-attackiert>
- Georg-August-Universität Göttingen/ Stabstelle Chancengleichheit (2020): Diskriminierungsschutz im Digitalen Lernen und Lehren. www.uni-goettingen.de 30. Oktober 2020. Online: <https://www.uni-goettingen.de/de/diskriminierungsschutz+im+digitalen+lehren+und+lernen/628987.html>
- Georg-August-Universität Göttingen/ Team Digitales Lernen und Lehren (2020): Nutzung von Zoom. Handreichung für Studierende. www.uni-goettingen.de 27. April 2020. Online: <https://www.uni-goettingen.de/de/document/download/351a7a63d4ab1faaac6e656bf68e20d9.pdf/Handreichung%20f%C3%BCr%20Studierenden%20zur%20Nutzung%20von%20Zoom.pdf>
- Georg-August-Universität Göttingen/ Team Digitales Lernen und Lehren (2020): Persönlichkeitsrecht Bild- /Tonaufnahmen. www.uni-goettingen.de 27. April 2020. Online: <https://www.uni-goettingen.de/de/document/download/2f28b812ba3b3687b188f539b4ca7d16.pdf/Handreichung%20zu%20Aufzeichnungen.pdf>
- Gleichstellungsbüro der RUB und Zentrum Wissenschaftsdidaktik (2021): Hinweise und Empfehlungen zu diskriminierungsfreier Lehre über den Videokonferenzanbieter Zoom. Handreichung. www.rub.de Januar 2021. Online: <https://el.rub.de/corona/wp-content/uploads/2021/01/Diskriminierungsfreie-Lehre-in-Zoom.pdf>

³ Ein ganz besonderer Dank gilt dem Hessischen Demokratiezentrum für erste Informationen und Hinweise auf Leitfäden!

- Heinke, Christian, Mary Shnayien, Florian Sprenger und Uwe Wippich (2020). Lehre unter besonderen Bedingungen. Leitfaden zur temporären Umstellung der Lehre auf Online-Formate. www.mediarep.org. Online: <https://mediarep.org/handle/doc/14513>.
- LHM/MBR (2014): Veranstaltungsstörungen durch die extreme Rechte ...und was dagegen hilft. www.muenchen.de/gegen-rechtsextremismus 2014. Online: https://www.lks-bayern.de/fileadmin/user_upload/user_upload/beratung/fuer_kommunalpolitik_und_verwaltung/Veranstaltungssto_rungen_durch_die_extreme_Rechte.pdf
- MBR und VDK Berlin (2010): Wir lassen uns nicht das Wort nehmen. Empfehlungen zum Umgang mit rechtsextremen Besucher/innen bei Veranstaltungen. www.mbr-berlin.de. Online: https://mbr-berlin.de/wp-content/uploads/2021/03/2010_mbr_hr-wort_web.pdf
- Mrasek, Volker (2018). Ein Jahr Science March - Willkür im Weißen Haus hält an. www.Deutschlandfunk.de, 13. April 2018. Online: https://www.deutschlandfunk.de/ein-jahr-science-march-willkuer-im-weissen-haus-haelt-an.676.de.html?dram:article_id=415525.
- Riehl, Ingo (2020): Zoom für unterbrechungsfreie Meetings einstellen. www.cms.hu-berlin.de (Computer und Medienservice) 6. Mai 2020. Online: <https://www.cms.hu-berlin.de/de/dl/multimedia/bereiche/tele/zoom/aufzeichnung/zoomunterbrechungsfrei.pdf>
- Rewa, Jeanne (2020): Dealing with disruptors in Zoom online meetings or trainings. www.trainingforchange.org 15. April 2020. Online: https://www.trainingforchange.org/training_tools/dealing-with-disruptors-online/
- Rosa Luxemburg Stiftung (2017): Haltung zeigen! Gesprächsstrategien gegen Rechts. www.rosalux.de. Online: <https://www.rosalux.de/publikation/id/37599/haltung-zeigen/>
- Stubbe, Julian (2020). Wieso Verschwörungstheorien die gesellschaftliche Akzeptanz wissenschaftlichen Wissens gefährden können – und was die Governance von Wissenschaft und Innovation dagegen tun kann. In: Volker Wittpahl/Institut für Innovation und Technik (Hg.): *Verschwörungstheorien und Wissenschaftsfeindlichkeit*. Berlin: iit, S. 13–14.
- Universität Frankfurt/ Gleichstellungsbüro (2020): Handreichung für eine diversitätsbewusste digitale Lehre. www.uni-frankfurt.de 29. April 2020. Online: https://www.uni-frankfurt.de/92255827/2020_04_29_DiversitDigitaleLehreHandreichung.pdf