Sichere Nutzung von Video-/Webkonferenz-Tools

Der Einsatz von Video-/Webkonferenz-Tools ist nicht nur in Krisen-Zeiten ein wertvolles Hilfsmittel, um Besprechungen und Gremiensitzungen durchzuführen und digitale Lehrformate anzubieten.
Damit Sie bei der Auswahl und Nutzung solcher Systeme arbeits- und datenschutzrechtlich auf der sicheren Seite sind, haben wir die wichtigsten Dinge für Sie zusammengefasst:

Auswahl eines Video-/Webkonferenz-Tools

- Da bei einem von der Hochschule unterstützten Einsatz von Video-/Webkonferenz-Anwendungen insbesondere auch der Schutz personenbezogener Daten zu gewährleisten ist, unterstützt die Hochschule derzeit nur die browser-basierten Webkonferenz-Anwendungen DNFconf sowie Cisco WebEx, die wie folgt zur Nutzung empfohlen werden:

Dienst	Teilnehmerzahl	empfohlene Nutzung
DFNconf	max. 23 (+50 Audio)	Gremiensitzungen, insbesondere mit vertraulichen Inhalten (Berufungskommissionen, Bewerbungsgespräche)
Cisco WebEx	max. 1.000	Vorlesungen und Seminare sowie virtuelle Meetings, Lern- und Projektgruppen mit Interaktionsmöglichkeit, Einzel- oder Gruppenunterricht sowie Sprechstunden bei Lehrenden

- Die Nutzung anderer gängiger Systeme kann die Hochschule aufgrund der vorhandenen technischen Ausstattung, der personellen Kapazitäten, aber auch aus datenschutzrechtlichen Gesichtspunkten derzeit nicht unterstützen. Daher sollten Sie für jegliche dienstliche sowie lehr- und studienbezogene Online-Kommunikation von der Nutzung solcher Programme absehen.

- Sollten Sie im Einzelfall und insbesondere für künstlerische Lehrangebote eine Nutzung besonders dafür geeigneter Tools (JamKazam, Doozzoo) in Erwägung ziehen, ist dies – auch zu Ihrer eigenen Absicherung – nur mit ausdrücklichem Einverständnis der Studierenden möglich, das durch eine schriftliche Einwilligung der Studierenden zu dokumentieren ist.
  Bitte beachten Sie jedoch, dass die Nutzung solcher Tools grundsätzlich in eigener Verantwortlichkeit geschieht und weder technisch noch rechtlich durch die Hochschule abgesichert werden kann.

Organisatorische Absicherung einer Webkonferenz

- Vor der Durchführung einer Webkonferenz ist eine Person als Veranstalter/in zu bestimmen, die als Einlader/in fungiert und über entsprechende Administratorenrechte verfügt.

- Gleichzeitig ist (im Team, mit Vorgesetzten, ggf. nach datenschutzrechtlicher Beratung) festzulegen, welche Daten übermittelt und gespeichert werden dürfen (Logfiles, Chatverläufe, Dokumente).

- Alle Teilnehmer der Webkonferenz sind durch den/die Veranstalter/in des Meetings vorab, also im Rahmen der Einladung oder spätestens auf der Login-Seite, über die Datenübermittlung und –nutzung zu informieren. Dies erfolgt durch einen Hinweis auf das genutzte Programm einschließlich einer Verlinkung auf die Datenschutzerklärungen des Anbieters sowie der Hochschule.

Technische Absicherung einer Webkonferenz

- Alle Teilnehmer benötigen einen Rechner, eine Webkamera und idealerweise ein Headset, sowie eine stabile Internetverbindung.

- Halten Sie Ihre Webkonferenz-Anwendungen immer aktuell und installieren Sie mögliche Updates.

- Bei der Vorbereitung einer Webkonferenz ist durch den/die Veranstalter/in zu beachten, dass datensparsame Voreinstellungen vorgenommen, nicht notwendige Funktionalitäten ausgeschaltet und notwendige Zugangsbeschränkungen genutzt werden. Dazu gehören insbesondere:
  - ✓ das Ausschalten von Trackingfunktionen, um eine unzulässige Überwachung von Arbeitnehmern und deren Arbeitszeiten zu verhindern (Anwesenheits-/Aktivitätsstatus, Aufmerksamkeitstracking),
  - ✓ das Nutzen von Zugangsbeschränkungen durch die Verwendung eines Passworts oder der Warteraumfunktion, damit sich unerwünschte oder unberechtigte Zuhörer nicht einwählen können, Es wird empfohlen, ein Meeting „zu schließen", wenn alle Teilnehmer im Meeting sind, so dass sich – selbst in Kenntnis eines Passworts – keine weitere Person einwählen kann.
  - ✓ die technische Minimierung der Übertragung nicht notwendiger Daten,
    z. B. durch Unkenntlichmachung des Hintergrunds der Webcam-Aufnahme (ausgrauen, verschwimmen) oder durch Begrenzung der Anzeige beim Desktop-Sharing auf notwendige Inhalte,
  - ✓ das Absehen von Aufzeichnungen eines Web-Meetings,
    Die Teilnehmer sollten generell gehalten sein, sich anderweitig Notizen zu machen, eine/n Protokollführer/in zu bestimmen und ein schriftliches Protokoll zu fertigen oder sich Dokumente und Präsentationen im Nachgang per E-Mail oder anderen sicheren Kanälen zur Verfügung zu stellen. Sollte einstimmig eine Aufzeichnung des Meetings vereinbart werden, ist hierfür eine schriftliche Einwilligung aller Teilnehmer erforderlich.
  - ✓ das Löschen zulässiger Aufzeichnungen, Chatverläufe und anderer Dokumentationen aus dem Konferenz-Tool nach dem Meeting.

  Soweit solche Voreinstellungen bereits durch die Zentrale IT vorgenommen wurden, sollten sie nicht ohne Rücksprache geändert werden.

- Geben sie bei größeren Gruppen Teilnehmende gezielt zum Sprechen frei (evtl. 2. Moderator der sich nur um die Struktur und Organisation Ihres virtuellen Raumes kümmert).

- Zur Verbesserung der Bild- und Tonqualität einer Webkonferenz wird empfohlen
  - ✓ Störquellen im Raum zu minimieren (Telefon stummschalten, Fenster und Tür schließen),
  - ✓ das Mikrofon stumm zu schalten, wenn Sie längere Zeit nichts sagen möchten,
  - ✓ ein Headset für eine bessere Sprachverständlichkeit und Audioqualität zu nutzen,
  - ✓ für eine ausreichende Beleuchtung Ihres Arbeitsplatzes zu sorgen (Gegenlicht-Situationen, wie ein Fenster oder einen angestrahlten weißen Hintergrund vermeiden),
  - ✓ die Kamera über oder direkt neben dem Bildschirm zu platzieren, um die Blickachse zu erhalten.

Ansprechpartner

Technische Fragen:	IT-Abteilung	support@hfm-weimar.de
(Datenschutz)rechtliche Fragen:	Justiziariat | Datenschutz	datenschutz@hfm-weimar.de