

Einwilligungserklärungen und Kenntnisnahmen

Inhalt:

- Nutzungsordnung zur Nutzung der IT-Infrastruktur
- Nutzungsumfang MS 365 Education
- Nutzungsordnung MS 365 Education
- Einwilligungserklärung zur Übertragung des Unterrichts aus dem Klassenzimmer

Nutzungsordnung zur Nutzung der IT-Infrastruktur und des Internetzugangs an Schulen

Gemäß KMBek vom 14.07.2022 IT-Infrastruktur und Internetzugang

I. Allgemeines und Geltungsbereich

Die Staatliche Fachoberschule und Berufsoberschule Erlangen gibt sich für die Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs sowie für die Nutzung von im Verantwortungsbereich der Schule stehenden Cloudangeboten (einschließlich digitaler Kommunikations- und Kollaborationswerkzeuge) folgende Nutzungsordnung. Sie gilt für Schülerinnen und Schüler, Lehrkräfte und sonstiges an der Schule tätiges Personal (siehe II.12).

II. Nutzungsregelungen

1. Allgemeine Regeln

Die schulische IT-Infrastruktur darf nur verantwortungsvoll und rechtmäßig genutzt werden. Insbesondere sind die Vorgaben des Urheberrechts und die gesetzlichen Anforderungen an Datenschutz und Datensicherheit zu beachten.

Persönliche Zugangsdaten müssen geheim gehalten werden. Die Verwendung von starken, d. h. sicheren Passwörtern wird empfohlen. Detaillierte Empfehlungen zu Länge und Komplexität von Passwörtern finden sich auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Bei dem Verdacht, dass Zugangsdaten bekannt geworden sind, muss das entsprechende Passwort geändert werden. Das Arbeiten unter fremden Zugangsdaten sowie die Weitergabe des Passworts an Dritte ist verboten.

Bei der Konfiguration sind weitere Sicherheitsvorkehrungen wie z. B. Verzögerungen, IP-Sperren im erforderlichen Umfang zu berücksichtigen.

Es dürfen keine Versuche unternommen werden, technische Sicherheitsvorkehrungen wie Webfilter oder Passwortschutz zu umgehen.

Auffälligkeiten, die die Datensicherheit betreffen, müssen an [datenschutz@fosbos-erlangen.de] gemeldet werden. Dies betrifft insbesondere öffentlich gewordene Passwörter oder falsche Zugangsberechtigungen.

2. Eingriffe in die Hard- und Softwareinstallation

Der unerlaubte Eingriff in die Hard- und Softwareinstallation und -konfiguration ist verboten. Dies gilt nicht, wenn Veränderungen auf Anordnung der Systembetreuerin oder des Systembetreuers durchgeführt werden oder wenn temporäre Veränderungen im Rahmen des Unterrichts explizit vorgesehen sind.

Private Endgeräte und externe Speichermedien dürfen nur mit Zustimmung des Systembetreuers oder einer aufsichtführenden Person an die schulische IT-Infrastruktur oder das Schul- sowie Verwaltungsnetz angeschlossen werden.

3. Anmeldung an den schulischen Endgeräten im Unterrichtsnetz

Zur Nutzung der von der Schule zur Verfügung gestellten IT-Infrastruktur und zur Nutzung bestimmter Dienste (z. B. Cloudangebote, Lernplattformen, Zugriff auf persönliches Netzlaufwerk) ist eine individuelle Anmeldung mit Benutzernamen und Passwort erforderlich. Nach Beendigung der Nutzung haben sich die Nutzerinnen und Nutzer abzumelden.

Der Anmeldevorgang in das jeweilige WLAN-Netzwerk wird unter III.2 spezifiziert.

4. Anmeldung im Verwaltungsnetz

Im Verwaltungsnetz werden besonders schützenswerte Daten verarbeitet. Daher ist eine benutzerspezifische Authentifizierung notwendig (z. B. Benutzername und Passwort). Die Berechtigungen werden nach Maßgabe von Aufgaben und Erfüllung schulischer Zwecke verteilt.

5. Protokollierung der Aktivitäten im Schulnetz

Es findet keine regelmäßige Protokollierung der Aktivitäten der Schülerinnen und Schüler sowie der Lehrkräfte und des sonstigen an der Schule tätigen Personals innerhalb des Schulnetzes statt. Es ist der Systembetreuung in Absprache mit der Schulleitung dennoch aus begründetem Anlass gestattet, vorübergehend eine Protokollierung zu technischen Zwecken durchzuführen, z. B. zur Erkennung von Bandbreitenengpässen, der Überprüfung der Funktionsfähigkeit des Schulnetzes oder der Sicherheitsanalyse der schulischen IT-Infrastruktur, vgl. Art. 6 Abs. 1 S.1 lit. e) DSGVO i. V. m. Art. 85 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG).

Die dadurch erzeugten Daten werden nach Abschluss der Analysen unwiderruflich gelöscht.

6. Speicherplatz innerhalb der schulischen IT-Infrastruktur

Beim Zugriff auf den für Nutzerinnen und Nutzern von der Schule zur Verfügung gestellte persönliche Speicherplatz innerhalb der schulischen IT-Infrastruktur ist eine Authentifizierung notwendig. Die Schule fertigt von diesem persönlichen Verzeichnis Sicherheitskopien (Backup) an.

Das IT-Infrastrukturnetzwerk ist aufgeteilt in die Teilnetze:

- Pädagogisches Netzwerk
- Verwaltungsnetzwerk

Pädagogischen Netzwerk:

Hier bietet die Schule eine klassenspezifische Austauschverzeichnisstruktur an, auf dem jede Schülerin und jeder Schüler sowie jede Lehrkraft mit Authentifizierung Daten bereitstellen kann. Dieses Austauschverzeichnis dient dem schnellen Datenaustausch während des Unterrichts.

Verwaltungsnetzwerk:

Im Verwaltungsnetzwerk gibt es Austauschverzeichnisse für Lehrkräfte. Diese dienen dem schnellen Datenaustausch. Für Verwaltungstätigkeiten existiert eine eigene Austauschverzeichnisstruktur, auf dem Verwaltungspersonal und Lehrkräfte mit besonderen Tätigkeiten Daten austauschen können.

7. Private Nutzung der schulischen IT-Infrastruktur

Die Schule gestattet den Schülerinnen und Schülern sowie den Lehrkräften und sonstigem an der Schule tätigen Personal in Abstimmung mit dem Schulaufwandsträger, geeignete Teile der schulischen IT-Infrastruktur (z. B. Internetzugang, Computer, Drucker) außerhalb des Unterrichts und anderer Lernzeiten für private Zwecke, z. B. zum Abruf von privaten Nachrichten oder zur privaten Recherche auf Webseiten, zu nutzen. Nicht erlaubt ist es, über den schulischen Internetzugang größere Downloads für private Zwecke durchzuführen.

Ein Anspruch auf Privatnutzung besteht nicht. Bei Missachtung der Nutzungsordnung oder anderweitigem Fehlverhalten kann das Recht auf Privatnutzung entzogen werden.

Jede Nutzerin bzw. jeder Nutzer ist selbst dafür verantwortlich, dass keine privaten Daten auf schulischen Endgeräten zurückbleiben.

8. Verbotene Nutzungen

Die rechtlichen Bestimmungen – insbesondere des Strafrechts, des Urheberrechts, des Datenschutzrechts und des Jugendschutzrechts – sind zu beachten. Es ist insbesondere verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen, zu speichern oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist beim Aufruf durch Schülerinnen und Schüler der Aufsicht führenden Person umgehend Mitteilung zu machen und anschließend die Anwendung unverzüglich zu schließen.

9. Besondere Verhaltensregeln im Distanzunterricht

Im Distanzunterricht sind bestimmte Verhaltensregeln zu beachten, um einen störungsfreien Unterricht sicherzustellen. Insbesondere beim Einsatz eines digitalen Kommunikationswerkzeugs sind geeignete Vorkehrungen gegen ein Mithören und die Einsichtnahme durch Unbefugte in Video- oder Telefonkonferenz, Chat oder E-Mail zu treffen, vgl. die vom Staatsministerium für Unterricht und Kultus (Staatsministerium) zur Verfügung gestellten Hinweise, abrufbar unter www.km.bayern.de/schule-digital/datensicherheit-an-schulen.html.

Zum Schutz der Persönlichkeitsrechte anderer Nutzerinnen und Nutzer ist zu gewährleisten, dass die Teilnahme oder Einsichtnahme unbefugter Dritter ausgeschlossen ist. Für die Anwesenheit von Erziehungsberechtigten, der Schulbegleitung, von Ausbilderinnen und Ausbildern, Kolleginnen und Kollegen oder sonstigen Personen in Videokonferenzen gilt: Soweit diese nicht zur Unterstützung aus technischen, medizinischen oder vergleichbaren Gründen benötigt werden und auch sonstige Gegebenheiten ihre Anwesenheit nicht zwingend erfordern (z. B. kein separater Raum für den Distanzunterricht, Aufsichtspflicht), ist ihre Beteiligung nicht zulässig.

10. Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs mit privaten Endgeräten

Die Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs mit privaten Endgeräten ist unter Einhaltung der Nutzungsordnung gestattet.

11. Besondere Vorschriften für Schülerinnen und Schüler

Die Nutzung der schulischen IT-Infrastruktur (Hard- und Software, Computer, Drucker, Scanner, Maus, Tastatur, ...) und des Internetzugangs durch Schülerinnen und Schüler ist an die schulischen Vorgaben

gebunden. Dies umfasst insbesondere die Pflicht, schulische Geräte sorgfältig zu behandeln, vor Beschädigungen zu schützen und – sofern erforderlich – für einen sicheren Transport mobiler Endgeräte zu sorgen. Störungen oder Schäden sind unverzüglich der Aufsicht führenden Person oder der benannten Ansprechpartnerin bzw. dem benannten Ansprechpartner zu melden. Wer schuldhaft Schäden verursacht, hat diese entsprechend den allgemeinen schadensersatzrechtlichen Bestimmungen des BGB zu ersetzen.

Jegliche Veränderungen der Installation und Konfiguration der von der Schule gestellten Computersysteme und des Netzwerkes (z.B. auch durch das Einschleusen von Viren, „Würmern“ oder „Trojanischen Pferden“) sowie Manipulationen an der schulischen Hardwareausstattung sind untersagt. Automatisch geladene Programme (z.B. Virens Scanner) dürfen nicht deaktiviert oder beendet werden.

Der Verzehr von Lebensmitteln und Getränken im Bereich der Computerarbeitsplätze ist nicht erlaubt.

Vor dem Verlassen des Raums bzw. PC-Bereichs sind die Geräte und der Arbeitsplatz ordnungsgemäß aufgeräumt und sauber zu hinterlassen. Dazu gehört das Ausrichten von Monitor, Tastatur und Maus, das Zurechtrücken des Stuhls und das Entfernen jeglichen Abfalls.

Bei grob fahrlässigen und vorsätzlichen Beschädigungen hat der Verursacher den Schaden und die u.U. nötigen Folgekosten zu ersetzen und ggf. strafrechtliche Konsequenzen zu tragen.

12. Besondere Vorschriften für Lehrkräfte und sonstiges an der Schule tätiges Personal

Die Nutzung der schulischen IT-Infrastruktur (Hard- und Software) und des Internetzugangs durch Lehrkräfte oder das sonstige an der Schule tätige Personal ist an die schulischen Vorgaben gebunden. Dies umfasst insbesondere die Pflicht, die schulischen Geräte sorgfältig zu behandeln, vor Beschädigungen zu schützen, und – sofern erforderlich – für einen sicheren Transport, insbesondere mobiler Endgeräte, zu sorgen. Jede Nutzerin bzw. jeder Nutzer ist im Rahmen gegebenenfalls bestehender Fortbildungspflichten gehalten, geeignete Fortbildungsangebote wahrzunehmen (vgl. § 9a Abs. 2 Lehrerdienstordnung - LDO).

Für den Umgang mit personalisierten mobilen Endgeräten, die Lehrkräften oder sonstigem an der Schule tätigen Personal zur Erledigung der dienstlichen Aufgaben zur Verfügung gestellt werden, gelten gesonderte Nutzungsbedingungen.

Störungen oder Schäden sind unverzüglich der Systembetreuung zu melden. Es gelten die Haftungsregeln des jeweiligen Dienst- bzw. Arbeitsverhältnisses, hilfsweise die allgemeinen Haftungsregeln.

III. Nutzungsbedingungen für den Internetzugang über das schulische WLAN

[Die folgenden Ausführungen gelten sinngemäß – soweit anwendbar – auch für Konstellationen, in denen sich die Nutzerinnen und Nutzer über LAN mit dem Netz verbinden.]

1. Gestattung zur Nutzung des kabellosen Internetzugangs (WLAN)

Die Schule stellt einen kabellosen Internetzugang (WLAN) zur Verfügung. Sie bietet der jeweiligen Nutzerin bzw. dem jeweiligen Nutzer für die Dauer des Aufenthaltes die Möglichkeit einer Mitbenutzung des Internetzugangs der Schule über WLAN. Dies gilt grundsätzlich unabhängig davon, ob der Zugriff über schulische oder private Geräte erfolgt. Die Nutzerin bzw. der Nutzer ist nicht berechtigt, Dritten die Nutzung dieses WLANs zu gestatten. Die zur Verfügung gestellte Bandbreite ist begrenzt. Es besteht kein Anspruch auf tatsächliche Verfügbarkeit, Eignung und Zuverlässigkeit des Internetzugangs.

Die Schule ist aus gegebenem Anlass jederzeit berechtigt, den Zugang der Nutzerin bzw. des Nutzers teil- oder zeitweise zu beschränken oder sie bzw. ihn von einer weiteren Nutzung ganz auszuschließen.

2. Zugang zum schulischen WLAN

Für Lehrkräfte und Verwaltungspersonal erfolgt der Zugang zum schulischen WLAN für Lehrkräfte über einen gemeinsamen Schlüssel (Pre-Shared-Key):

Die Schule stellt Lehrkräften sowie dem Verwaltungspersonal für die Mitbenutzung des Internetzugangs Zugangsdaten über einen gemeinsamen Schlüssel (Pre-Shared-Key) zur Verfügung (Zugangssicherung). Die Nutzerinnen und Nutzer haben dabei denselben Zugangsschlüssel, der über das digitale Lehrerzimmer bekannt gegeben wird. Diese Zugangsdaten dürfen nicht an Dritte weitergegeben werden. Die Schule kann diese Zugangsdaten jederzeit ändern bzw. in ihrer Gültigkeit zeitlich beschränken.

Für Schülerinnen und Schüler erfolgt der Zugang über ein Ticketsystem:

Die Schule stellt den Schülerinnen und Schülern für die Mitbenutzung des Internetzugangs Zugangsdaten über ein Ticketsystem zur Verfügung (Zugangssicherung). Diese Zugangsdaten können an einem Endgerät verwendet werden und sind nur für einen Monat gültig. Die Zugangsdaten dürfen nicht an Dritte weitergegeben werden und sind geheim zu halten. Bei Ungültigkeit der Zugangsdaten können neue Zugangsdaten angefordert werden.

3. Haftungsbeschränkung

Die Nutzung des schulischen WLANs erfolgt auf eigene Gefahr und auf eigenes Risiko der Nutzerin bzw. des Nutzers. Für Schäden an privaten Endgeräten oder Daten der Nutzerin bzw. des Nutzers, die durch die Nutzung des WLANs entstehen, übernimmt die Schule keine Haftung, es sei denn, die Schäden wurden von der Schule vorsätzlich oder grob fahrlässig verursacht.

Der unter Nutzung des schulischen WLANs hergestellte Datenverkehr verwendet eine Verschlüsselung nach dem aktuellen Sicherheitsstandard, so dass die missbräuchliche Nutzung Dritter verhindert wird und die Daten nicht durch Dritte eingesehen werden können. An unserer Schule werden die Datenströme des WLANs für Schülerinnen und Schüler durch einen Webfilter kontrolliert. Bei den Schülerleihgeräten (Surface-GO-Geräte) stehen keine zentralen Sicherheitsinstanzen zur Verfügung (Webfilter, Virenschutz o.a.).

Die Schule setzt geeignete Sicherheitsmaßnahmen ein, die dazu dienen, Aufrufe von jugendgefährdenden Inhalten oder das Herunterladen von Schadsoftware zu vermeiden. Dies stellt aber keinen vollständigen Schutz dar. Die Sicherheitsmaßnahmen dürfen nicht bewusst umgangen werden.

Die Schule stellt bei der Nutzung des schulischen Internetzugangs über private Endgeräte, sowie über die Schülerleihgeräte keine zentralen Sicherheitsinstanzen (z. B. Virenschutz o. ä.) zur Verfügung.

4. Verantwortlichkeit der Nutzerin bzw. des Nutzers

Für die über das schulische WLAN übermittelten Daten sowie die darüber in Anspruch genommenen Dienstleistungen und getätigten Rechtsgeschäfte ist die Nutzerin bzw. der Nutzer allein verantwortlich und hat etwaige daraus resultierende Kosten zu tragen.

Die Nutzerin bzw. der Nutzer ist verpflichtet, bei Nutzung des schulischen WLANs geltendes Recht einzuhalten. Insbesondere ist die Nutzerin bzw. der Nutzer dazu verpflichtet sich an folgende Vorgaben zu halten:

- Es ist verboten, urheberrechtlich geschützte Werke widerrechtlich zu vervielfältigen, zu verbreiten oder öffentlich zugänglich zu machen - dies gilt insbesondere im Zusammenhang mit der Nutzung von Streamingdiensten, dem Up- und Download bei Filesharing-Programmen oder ähnlichen Angeboten.
- Es ist verboten, sitten- oder rechtswidrigen Inhalte abzurufen oder zu verbreiten.
- Geltende Jugend- und Datenschutzvorschriften sind zu beachten.
- Es dürfen keine herabwürdigenden, verleumderischen oder bedrohenden Inhalte versendet oder verbreitet werden („Netiquette“).
- Es ist nicht gestattet, das WLAN zur Versendung von Spam oder Formen unzulässiger Werbung oder Schad-Software zu nutzen.
- Die Veröffentlichung von Fotos ist nur gestattet, wenn die betroffenen Personen bzw. bei Minderjährigen deren Erziehungsberechtigte ihr Einverständnis erklärt haben. Persönliche Daten von Schülern und Lehrkräften (z.B. Namen) dürfen nur mit der vorherigen Zustimmung des Betroffenen verwendet werden. Für fremde Inhalte ist das Urheberrecht zu beachten, d.h. fremde Texte, Logos, Bilder, Karten etc. dürfen nicht ohne ausdrückliche, schriftliche Genehmigung des Urhebers/der Urheberin auf eigenen Internetseiten verwendet werden.
- Grundsätzlich ist jede Schülerin/jeder Schüler für die von ihr/ihm erstellten Inhalte zivilrechtlich und strafrechtlich verantwortlich und kann ggf. entsprechend belangt werden. Die Schule ist nicht für Angebote und Inhalte Dritter verantwortlich, die über das Internet abgerufen werden können.

5. Freistellung des Betreibers von Ansprüchen Dritter

Die Nutzerin bzw. der Nutzer stellt den Bereitsteller des Internetzugangs von sämtlichen Schäden und Ansprüchen Dritter frei, die auf eine rechtswidrige Verwendung des schulischen WLANs durch die Nutzerin bzw. den Nutzer oder auf einen Verstoß gegen die vorliegende Nutzungsordnung zurückzuführen sind. Diese Freistellung erstreckt sich auch auf die mit der Inanspruchnahme bzw. deren Abwehr zusammenhängenden Kosten und Aufwendungen.

6. Protokollierung

Eine Protokollierung der Aktivitäten der einzelnen Nutzerinnen und Nutzer bei Nutzung des schulischen Internetzugangs erfolgt nicht.

IV. Schlussvorschriften

Diese Nutzungsordnung tritt am Tag nach ihrer ortsüblichen Bekanntgabe in Kraft. Einmal zu jedem Schuljahresbeginn findet eine Nutzerbelehrung statt, die für Schülerinnen und Schüler, Lehrkräfte und das sonstige an der Schule tätige Personal in geeigneter Weise dokumentiert wird.

- Die Einwilligungen/ Ablehnungen werden durch das Setzen von Häkchen und Unterschrift auf dem gesonderten Formular „Einwilligungserklärungen“ abgegeben!

Nutzungsumfang Microsoft 365-Education

- Das System stellt pro Klasse und unterrichtetem Fach einen (virtuellen) Kursraum zur Verfügung, für den jeweils ein Gruppenchat besteht. Der Benutzername ist nur von anderen Mitgliedern der Schule einsehbar, die ebenfalls Nutzerkonten in derselben Schule besitzt.
- Weiterhin bietet die Anwendung die Möglichkeit, in jedem Kursraum eine Video- oder Telefonkonferenz mit Teilnehmern des Kurses durchzuführen. Jeder Teilnehmer kann dabei wählen, ob sein Videobild übertragen wird oder nicht. Nur Lehrkräfte können Videokonferenzen initiieren. Jeder kann sein Videobild und seinen Ton jederzeit aktivieren oder deaktivieren (z. B. bei Nebengeräuschen). Weder Lehrkräften noch Schülerinnen oder Schülern wird es durch das System ermöglicht, Videokonferenzen aufzuzeichnen.
- Die Teilnahme an einer Telefon-/Videokonferenz ist auch mit einem (Festnetz-)Telefon möglich; somit ist die Verwendung eines digitalen Endgeräts nicht unbedingt erforderlich.
- Die Schülerinnen und Schüler sowie die Lehrkräfte einer Schule können untereinander via E-Mail kommunizieren. Ein E-Mail-Versand an Adressen außerhalb der jeweiligen Schulinstanz ist hingegen nicht möglich (sog. „closed campus“).
- Im Kursraum können die Nutzer Dateien (z. B. Textdokumente, Präsentationen, Audiodateien) bereitstellen.
- Die Nutzerinnen und Nutzer können gemeinsam und ggf. auch gleichzeitig an Dokumenten arbeiten.
Dazu stehen die gängigen Office-Anwendungen (Word, Excel, PowerPoint) zur Verfügung.
- Die Lehrkraft kann im Kursraum für die Schülerinnen und Schüler Aufgaben einstellen, die diese bearbeiten können. Die Lehrkraft kann dazu individuell Feedback abgeben.
- Die Anwendung kann über einen Internetbrowser genutzt werden. Daneben steht es den Nutzerinnen und Nutzern frei, die Anwendung über eine App für mobile Geräte zu nutzen (Android und iOS). Hierfür muss die Nutzerin oder der Nutzer sich für eine Installation der entsprechenden App entscheiden.

➔ Die Einwilligungen/ Ablehnungen werden durch das Setzen von Häkchen und Unterschrift auf dem gesonderten Formular „Einwilligungserklärungen“ abgegeben!

Nutzungsordnung von Microsoft 365-Education

Für die Verwendung von Microsoft 365 Education an der Staatlichen Fachoberschule Erlangen

Mit der Bereitstellung von Microsoft-365-Education leisten wir einen kostenfreien Beitrag für das gemeinsame Lernen im Unterricht und Zuhause.

1. Übersicht über die beinhaltenden Apps und Tools:

Schülerinnen und Schüler können über diesen Dienst verschiedene Microsoft-Produkte über die Dauer Ihres Schulbesuchs vollumfänglich nutzen. Die A1-Plus-Lizenz erlaubt sowohl neben der ausschließlichen Onlinenutzung ebenso die Nutzung von Office365 über die Microsoft-Apps.

| | |
|------------------------|--|
| Web-Apps / Apps: | <p>Webbasierte Dokumentenbearbeitung mit Word, Excel, PowerPoint. Auch als App nutzbar (z. B. Teams für Android und iOS).</p> <p>Office-Clientanwendungen: Word, Excel, PowerPoint, Outlook, ... (gleichzeitiges Arbeiten an Dokumenten mit individuellem Feedback durch die Lehrkraft möglich).</p> |
| Lizenzen und Endgeräte | <p>Die Office365-Lizenz ist auf bis zu 5 Endgeräten installierbar. Die E-Mail-Adressen der SuS sind nur innerhalb der Organisation erreichbar.</p> |
| Lernorganisation | <p>Tools zur Unterstützung und Organisation des Unterrichts für die Schule und Zuhause: Kursnotizbuch, Sway, Forms</p> |
| Cloud-Speicher | <p>Für die SuS steht ein Cloudspeicher zur Verfügung (ausschließlich für unterrichtsbezogene Inhalte).</p> |
| Speicherung/Löschung | <p>Nach der Beendigung der Schulzeit erlischt das Benutzerkonto der SuS. Damit werden alle von den SuS angelegten Daten und Informationen gelöscht.</p> |

2. Nutzungsbedingungen:

2.1 Anwendungsbereich

Diese Nutzungsbedingungen regeln die Nutzung des von der Schule bereitgestellten digitalen Kommunikationswerkzeugs Microsoft Office365 Apps for Students (im Folgenden: „Office365 und Teams“).

Sie gelten für alle Schülerinnen und Schüler, die Office365 und Teams nutzen, und gehen den daneben bestehenden EDV-Nutzungsbedingungen der Schule vor.

2.2 Zulässige Nutzung

Die Nutzung der Plattform ist nur für schulische Zwecke zulässig. Sie dient dazu, die aktuell notwendigen schulischen Kommunikations- und Lernangebote zu unterstützen und dabei das Angebot von mebis – Landesmedienzentrum Bayern sinnvoll zu ergänzen.

2.3 Anlegen von Konten für Schülerinnen und Schüler

Die Nutzung von Office365 und Teams ist für Schülerinnen und Schüler freiwillig. Nutzerkonten für Schülerinnen und Schüler werden nur angelegt, wenn Sie (bzw. bei Minderjährigen deren Erziehungsberechtigte) den Nutzungsbedingungen für Schülerinnen und Schüler zugestimmt und Ihr Einverständnis mit der damit verbundenen Datenverarbeitung erklärt haben. Bei Schülerinnen und Schülern zwischen 14 und 18 Jahren ist zusätzlich deren Zustimmung erforderlich.

2.4 Nutzung mit privaten Geräten

Die Nutzung von Office365 und Teams ist grundsätzlich über den Internetbrowser des Nutzer-Geräts möglich. Die Installation der Microsoft Teams-App ist nicht notwendig und erfolgt ggf. in eigener Verantwortung der Nutzerinnen und Nutzer.

2.5. Datenschutz und Datensicherheit

Beim Einsatz mobiler (privater) Geräte müssen diese mindestens durch eine PIN oder ein Passwort geschützt werden.

Das Gebot der Datenminimierung ist zu beachten: Bei der Nutzung sollen so wenig personenbezogene Daten wie möglich verarbeitet werden. Insbesondere das Entstehen nicht benötigter Schülerdaten beim Einsatz von Office365 und Teams ist zu vermeiden.

Die Aufzeichnung einer Bild-, Ton- oder Videoübertragung, z. B. durch eine Software oder das Abfotografieren des Bildschirms, ist nicht gestattet.

Die Kamera- und Tonfreigabe durch die Nutzerinnen und Nutzer erfolgt freiwillig. Es muss beachtet werden, dass es nicht ausgeschlossen werden kann, dass Dritte, die sich mit Nutzerinnen und Nutzern im selben Zimmer befinden (z.B. Haushaltsangehörige) den Bildschirm einer Nutzerin oder eines Nutzers und darauf abgebildete Kommunikationen einsehen können.

Sensible Daten gem. Art. 9 DSGVO (z. B. Gesundheitsdaten, rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetischen und biometrischen Daten) dürfen nicht verarbeitet werden.

Bei der Nutzung sind das Mithören und die Einsichtnahme durch Unbefugte zu verhindern. Die Nutzung der Videokonferenzfunktionen an öffentlichen Orten, insbesondere in öffentlichen Verkehrsmitteln, ist untersagt.

Die Zugangsdaten dürfen nicht an andere Personen weitergegeben werden. Wer vermutet, dass sein Passwort anderen Personen bekannt geworden ist, ist verpflichtet, dieses zu ändern. Die Verwendung eines fremden Nutzerkontos ist grundsätzlich unzulässig. Passwörter sind von anderen unbeobachtet einzugeben und dürfen nicht unverschlüsselt auf Rechnern gespeichert werden. Initialpasswörter und zurückgesetzte Passwörter sind vor der Nutzung der Dienste durch eigene Passwörter zu ersetzen.

Nach Beendigung der Nutzung haben sich die Nutzerinnen und Nutzer bei Office365 und Teams abzumelden.

Eine Verwendung des schulischen Nutzerkontos zur Authentifizierung an anderen Online-Diensten ist nicht zulässig, außer es ist ein von der Schule zugelassener Dienst.

2.6. Verbotene Nutzungen

Die Schülerinnen und Schüler sind verpflichtet, bei der Nutzung der Plattform geltendes Recht einzuhalten, u. a. das Strafrecht und das Jugendschutzrecht. Außerdem ist jede Nutzung untersagt, die beinhaltet, dass die berechtigten Interessen der Schule beeinträchtigt werden (z. B. Schädigung des öffentlichen Ansehens der Schule; Schädigung der Sicherheit der IT-Ausstattung der Schule).

Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Plattform abzurufen, zu speichern oder zu verbreiten. Von den Teilnehmerinnen und Teilnehmern über Office365 und Teams bereitgestellte Inhalte dürfen nicht unbefugt in sozialen Netzwerken oder sonstiger Weise verbreitet werden.

2.7. Verstoß gegen die Nutzungsbedingungen

Im Falle eines Verstoßes gegen diese Nutzungsbedingungen behält sich die Schulleitung das Recht vor, den Zugang zu Office365 und Teams zu sperren. Davon unberührt behält sich die Schulleitung weitere Maßnahmen vor.

2.8. Schlussbestimmungen

Tritt eine Schülerin oder ein Schüler während der Vertragslaufzeit aus einer angemeldeten Schule aus (beispielsweise durch Schulwechsel) und wird daher vom Schul-Administratoren das Nutzerkonto dieser Person entfernt, wird dieses nach spätestens 30 Tagen unwiderruflich gelöscht. Daneben gibt es die Möglichkeit, Nutzerkonten direkt zu löschen.

→ Die Einwilligungen/ Ablehnungen werden durch das Setzen von Häkchen und Unterschrift auf dem gesonderten Formular „Einwilligungserklärungen“ abgegeben!

Einwilligungserklärung zur Übertragung des Unterrichts aus dem Klassenzimmer

Übertragung des Videobilds der im Klassenzimmer anwesenden Schülerinnen und Schüler

Mit einer Übertragung des Unterrichts aus dem Klassenzimmer können Schülerinnen und Schüler, Lehrkräfte sowie Studienreferendarinnen und -referendare bzw. Lehramtsanwärterinnen und -anwärter im Rahmen von Unterrichtsbeeinträchtigungen (COVID-19, wetterbedingte Schulschließung, ...) trotz räumlicher Trennung in das Unterrichtsgeschehen vor Ort eingebunden werden.

Bei der Übertragung aus dem Klassenzimmer gilt:

- Die Online-Übertragung aus dem Klassenzimmer erfolgt zur Erfüllung des Bildungs- und Erziehungsauftrags der Schule.
- Eine Aufzeichnung der Übertragung durch die Schule findet nicht statt. Genauso ist eine Aufzeichnung der Übertragung durch im Distanzunterricht befindliche Schülerinnen und Schüler sowie Lehrkräfte untersagt.

Zur Online-Übertragung aus dem Klassenzimmer setzt unsere Schule MS Teams als Videokonferenztool ein.

→ Die Einwilligungen/ Ablehnungen werden durch das Setzen von Häkchen und Unterschrift auf dem gesonderten Formular „Einwilligungserklärungen“ abgegeben!