Version 01.09.2023

Einwilligungserklärung

Inhalt

Ich habe/wir haben die Nutzerordnung des Gymnasium Allermöhe (https://gymall.de/privacy/) gelesen. Ich/wir erkläre mich/erklären uns mit den darin enthaltenen Nutzungsbedingungen einverstanden.

Mir/uns ist bekannt, dass ich/wir jeweils nur einen Eltern-Account bekommen kann/können, wenn mindestens eines meiner Kinder einen IServ-Account besitzt. Besitzt keines meiner Kinder mehr einen IServ-Account an dieser Schule, ist der Eltern-Account automatisch nicht mehr verfügbar.

Mir/uns ist bekannt, dass ich/wir diese Einwilligungserklärung jederzeit ohne nachteilige Folgen widerrufen kann/können. Eine Nicht-Einwilligung hat keine Nachteile für unser Kind oder mich/uns. Eine Nutzung von IServ und anderen digitalen Zugängen ist dann allerdings ausgeschlossen.

Informationen zu den Modulen, die Ihre Schule einsetzten kann und den dort verarbeiteten Daten finden Sie im Detail in dem Dokument „Welche Daten werden in welchem Modul verarbeitet.docx“, dass Ihnen die Schule gern übergibt. Sie finden es auch unter https://www.iserv.de/downloads/privacy/ im Dokumentenpaket für Schulen.

_____

Ort, Datum

_____

Unterschrift Erziehungsberechtigte(r)[1]

_____

Unterschrift Erziehungsberechtigte(r)[1]

_____

Unterschrift Schüler/Schülerin[2]

1 bei Schülerinnen und Schülern bis zur Vollendung des 18. Lebensjahrs
2 bei Schülerinnen und Schülern ab Vollendung des 15. Lebensjahrs

Benutzerordnung für die Nutzung von IServ am Gymnasium Allermöhe[3]

Präambel

Die Schule stellt ihren Schülerinnen, Schülern und Lehrkräften und anderen Mitarbeitern (im Folgenden: Nutzer) als Kommunikations- und Austauschplattform IServ zur Verfügung.

Diese Plattform kann mit einem eigenen Zugang sowohl über die PCs im lokalen Schulnetzwerk als auch von jedem Computer bzw. Handy mit Internetzugang außerhalb der Schule genutzt werden.

Diese Benutzerordnung enthält verbindliche Regeln für die Nutzung der Plattform IServ für alle Nutzer.

IServ dient im pädagogischen Netzwerk ausschließlich der schulischen Kommunikation und ermöglicht allen Nutzern, schulbezogene Daten zu speichern und auszutauschen. Alle Nutzer verpflichten sich, die Rechte anderer Personen zu achten.

Nutzungsmöglichkeiten

Die Schule entscheidet darüber, welche IServ-Module wann für den innerschulischen Gebrauch freigeschaltet werden und welcher Nutzerkreis zu diesem Zugang erhält. Um IServ nutzen zu können, ist eine Einwilligung des Nutzers / der Erziehungsberechtigten notwendig.

In der Regel dürfen *besondere Arten personenbezogener Daten* (sensible Daten) mit dem IServ Schulserver nicht verarbeitet werden, da diese einem erhöhten Schutzniveau unterliegen. Details regelt das Schulgesetz / die für die Schule gültigen Verordnungen.

Netiquette

Für die auf der IServ-Plattform zur Verfügung gestellten Messenger-Rooms und Foren gelten folgende Regeln:

- Alle Benutzer verpflichten sich zu einer respektvollen Kommunikation miteinander.
- Verboten sind rassistische, pornographische oder Gewalt verherrlichende Äußerungen oder Bilder / Videos.
- Die Verwendung irreführender Nicknames ist untersagt.
- Meinungsverschiedenheiten sind wie üblich sachlich auszutragen.
- Persönliche Beleidigungen sind nicht zulässig.
- Ganze Wörter oder Sätze in Großbuchstaben stehen im Messenger/Chat für lautes Schreien. Das ist unhöflich und in den Chats und Foren unserer Schule nicht nicht erwünscht.
- Das Gleiche gilt für das endlose Wiederholen von Sätzen, URLs oder sinnloser Zeichenfolgen.
- Racheaktionen und private Streitereien haben nichts im Chat zu suchen und werden geahndet.

Passwörter

Jeder Nutzer erhält ein Nutzerkonto. Das Nutzerkonto muss durch ein nicht zu erratendes Passwort von mindestens acht Zeichen Länge (Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen) gesichert werden. Es ist untersagt, das Passwort anderen Nutzern mitzuteilen. Erfährt ein Nutzer, dass jemand unberechtigt Kenntnis von seinem Passwort hat, so muss er sein Passwort unverzüglich ändern.

Sollte ein Nutzer sein Passwort vergessen haben, ist er verpflichtet, das durch einen Administrator neu vergebene Passwort möglichst sofort zu ändern.

Zusätzlich zum Passwort kann die Schule auch eine 2-Faktor-Authentifizierung für IServ einrichten.

Alle Nutzer sind verpflichtet, ggf. eingesetzte Filter und Sperren zu respektieren und diese nicht zu umgehen.

3 Quelle: https://iserv.de/downloads/privacy/, Version 1.9, Stand 27.03.2023

Die Sicherung eigener in IServ gespeicherter Dateien gegen Verlust obliegt der Verantwortung der Nutzer, da eine Rücksicherung mit unverhältnismäßigem Aufwand verbunden wäre.

Das Senden, Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte ist auf dem Schulserver ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten. Die Schule übernimmt keine Verantwortung für die Inhalte und die Art gespeicherter Daten. Weil umfangreiche Up- und Downloads die Arbeitsgeschwindigkeit des Servers beeinträchtigen, sind diese nicht erlaubt. Die Installation oder Nutzung fremder Software darf und kann nur von den Administratoren durchgeführt werden. Ausnahmen sind vorab mit den Administratoren abzusprechen.

Administratoren

Die Administratoren haben weitergehende Rechte, verwenden diese aber grundsätzlich nicht dazu, sich Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen. Dies ist durch eine schriftliche Vereinbarung geregelt.

Protokolle

Das IServ-System erstellt Log-Dateien (Protokolle), die in schwerwiegenden Fällen (z.B. bei Regelverstößen, Betrugs- und Täuschungsversuchen oder Rechtsverstößen) auf Weisung der Schule ausgewertet werden können.

Festplattenbereich

Jeder Benutzer erhält einen Festplattenbereich mit einem von der Schule definierten Speicherkapazität, der zum Speichern von Mails und unterrichtsbezogenen Dateien genutzt werden kann. Eine anderweitige Nutzung ist nicht gestattet.

Hausaufgaben

Hausaufgaben können über IServ gestellt werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum, die Schüler sind verpflichtet, in angemessenen Abständen zu prüfen, ob es Neuigkeiten gibt.

Verhaltensregeln zu einzelnen IServ-Modulen

E-Mail

Soweit die Schule den Nutzern (Schülerinnen und Schüler) einen persönlichen E-Mail-Account zur Verfügung stellt, darf dieser nur für die interne schulische Kommunikation verwendet werden. Die Schule ist kein Anbieter von Telekommunikation im Sinne von §3 Nr. 6 Telekommunikationsgesetz. Ein Rechtsanspruch der Nutzer auf den Schutz der Kommunikationsdaten im Netz besteht gegenüber der Schule somit grundsätzlich nicht. Die Inhalte der Mails und welche personenbezogenen Daten in IServ verarbeitet werden dürfen, müssen sich an den für unser Bundesland geltenden Schulgesetz orientieren.

Die schulische E-Mail-Adresse darf nicht zur Anmeldung bei Internetadressen jeglicher Art verwendet werden. Das gilt insbesondere für alle sozialen Netzwerke (Facebook, Instagram).

Die Schule ist berechtigt, im Falle von konkreten Verdachtsmomenten von missbräuchlicher oder strafrechtlich relevanter Nutzung des E-Mail-Dienstes die Inhalte von E-Mails zur Kenntnis zu nehmen. Die betroffenen Nutzer werden hierüber unverzüglich informiert.

Soweit die Schule den Nutzern (Lehrkräfte Mitarbeiter) einen persönlichen E-Mail-Account zur Verfügung stellt, der auch eine Kommunikation mit Kommunikationspartnern außerhalb der Schule zulässt (interner und externer Gebrauch), ist folgendes zu beachten:

Der E-Mail-Account wird nur für den Austausch von Informationen im schulischen Zusammenhang bereitgestellt. Insbesondere darf der schulische E-Mail-Account nicht zur privaten Nutzung von Internetangeboten wie sozialen Netzwerken wie Facebook oder Twitter verwendet werden.

Die Schule ist damit kein Anbieter von Telekommunikation im Sinne von § 3 Nr. 6 Telekommunikationsgesetz. Ein Rechtsanspruch der Nutzer auf den Schutz der Kommunikationsdaten im Netz besteht gegenüber der Schule somit grundsätzlich nicht. Die Schule ist berechtigt, im Falle von konkreten Verdachtsmomenten von missbräuchlicher oder strafrechtlich relevanter Nutzung des E-Mail-Dienstes die Inhalte von E-Mails zur Kenntnis zu nehmen. Die betroffenen Nutzer werden hierüber unverzüglich informiert.

Die Inhalte der Mails und welche personenbezogenen Daten in IServ verarbeitet werden dürfen, müssen sich an den für unser Bundesland geltenden Schulgesetz orientieren.

Private Kommunikation mit anderen Personen über diesen schulischen E-Mail-Account ist deshalb zu vermeiden, da nicht ausgeschlossen werden kann, dass die Inhalte von E-Mails Dritter durch Einsichtnahmen der Schule zur Kenntnis genommen werden.

Der massenhafte Versand von E-Mails, sowie E-Mails, die dazu gedacht sind, andere Nutzer über Absender oder Glaubhaftigkeit der übermittelten Nachricht zu täuschen, sind verboten.

Forum

Soweit die Schule eine Forum-Funktion zur Verfügung stellt, gelten dieselben Vorgaben wie bei der E-Mail-Nutzung. Öffentliche Foren stehen allen registrierten IServ-Benutzern offen, während Gruppenforen nur von den jeweiligen Gruppenmitgliedern genutzt werden können. Darüber hinaus sind die Moderatoren der Foren berechtigt, unangemessene Beiträge zu löschen oder zu bearbeiten. Von „außen", d.h. für nichtregistrierte IServ-Benutzer sind diese Bereiche nicht zugänglich.

Kalender

Kalendereinträge für Gruppen werden nach bestem Wissen eingetragen und nicht manipuliert.

Messenger

Soweit die Schule die Messenger-Funktion zur Verfügung stellt, gelten dieselben Vorgaben wie bei der E-Mail-Nutzung.

Videokonferenzen

Sofern die Schule das Modul einsetzt, werden die Nutzer mit einer separaten Nutzungsordnung über das Verfahren informiert. Auch eine eigene Einwilligung ist dann notwendig.

Verstöße

Im Fall von Verstößen gegen die Nutzungsordnung kann das Konto temporär oder permanent gesperrt werden. Damit ist die Nutzung schulischer Computer sowie die Nutzung von IServ auf schulischen und privaten Geräten nicht mehr möglich.

Unabhängig davon besteht die Möglichkeit, Nutzern den Zugang zu einzelnen Komponenten oder Modulen zu verweigern, sodass beispielsweise das Anmelden am Schul-WLAN nicht mehr möglich ist, aber auf Schul-Computern und Zuhause IServ weiterhin genutzt werden kann.

Die Ahndung von Verstößen liegt im Ermessen der Schulleitung.

Elternaccounts

Sofern das Modul der Elternregistrierung eingesetzt wird, geschieht das nur, wenn die Eltern in diese Verarbeitung ihrer Daten einwilligt und sich mittels eines von der Schule gestellten Codes angemeldet haben. Ein Elternkonto kann nur fest verbunden mit einem Schülerkonto erstellt werden. Für die Berechtigungen eines Eltern-Accounts ist die Schule verantwortlich.

Änderungen der Nutzungsordnung und Einwilligungserklärung

Hinweise zu Änderungen

1. Die Erziehungsberechtigten erklären sich damit einverstanden, dass die Schule zukünftige Änderungen dieser Nutzungsordnung und Einwilligungserklärung elektronisch und/oder online kommuniziert.
2. Änderungen werden rechtzeitig im Voraus angekündigt, um den Erziehungsberechtigten ausreichend Zeit zu geben, sich mit den neuen Bedingungen vertraut zu machen.

Zustimmung zu Änderungen

1. Die Erziehungsberechtigten erhalten mit der Bekanntgabe von Änderungen eine angemessene Übergangsfrist, innerhalb der sie den geänderten Bedingungen zustimmen müssen.
2. Sollten die Erziehungsberechtigten den geänderten Bedingungen nicht zustimmen, bemüht sich die Schule, gemeinsam mit den Erziehungsberechtigten eine alternative Lösung zu finden). Ist dies nicht möglich werden alle zugehörigen Zugänge eingestellt.
3. Die Schule stellt sicher, dass den Schülerinnen und Schülern durch die Einstellung des Zugangs keine Nachteile entstehen.
4. Die Schülerinnen und Schüler werden durch ihre Erziehungsberechtigten vertreten und können rechtlich nicht alleine zustimmen.

Fortgeltung der übrigen Bestimmungen

Die übrigen Bestimmungen dieser Nutzungsordnung und Einwilligungserklärung bleiben von Änderungen unberührt und behalten ihre Gültigkeit, sofern sie nicht ausdrücklich geändert oder aufgehoben werden.

WebUntis: digitaler Stunden- und Vertretungsplan[4]

Datenschutzrechtliche Informationen nach Art. 13 DS-GVO

An dem Gymnasium Allermöhe nutzen Schüler, Eltern und Lehrkräfte WebUntis als digitalen Stunden- und Vertretungsplan. Damit das möglich ist, werden auch personenbezogene Daten der Benutzer verarbeitet, von der Schule und von **WebUntis GmbH/ Hamburger Behörde für Schule und Berufsbildung (BSB)**. Hiermit möchten wir Ihnen / dir alle wichtigen Informationen dazu geben.

Ausführliche Informationen

Informationen in vereinfachter Darstellung.

Für wen gelten diese Datenschutzhinweise?

Diese Informationen zur Datenverarbeitung im Zusammenhang mit der Nutzung von WebUntis gelten für alle schulischen Nutzer von WebUntis, Schüler, Eltern und Lehrkräfte.

Diese Informationen sind für alle WebUntis Benutzer der Schule.

Wer ist für die Verarbeitung meiner Daten verantwortlich und an wen kann ich mich zum Thema Datenschutz wenden?

Gymnasium Allermöhe, Walter-Rothenburg-Weg 41, 21035 Hamburg, Olaf Colditz
Olaf Colditz, Olaf.Colditz@bsb.hamburg.de

Wenn du Fragen zum Schutz deiner Daten hast oder Probleme auftreten, rede mit diesen Personen.

Welche Daten werden verarbeitet und woher kommen sie?

Bei der Nutzung von WebUntis über Browser oder App geht es um folgende personenbezogene Daten:

1. Anmeldedaten (Benutzer, Passwort) werden für jeden Nutzer von der Schule erstellt.
2. Die Zuordnung zu Gruppen und die damit verbundenen Rollen und Rechte, die Spracheinstellung und der Kontostatus erfolgen anhand von Informationen aus der Schulverwaltung.
3. Weitere Daten entstehen bei der Nutzung von WebUntis zum Abrufen des digitalen Stunden- und Vertretungsplans. Das sind:
    a. Server-Logdaten (z.B. Browsertyp und -version, Betriebssystem, IP Nummer)
    b. Von WebUntis erhobene Nutzungsdaten (IP Adresse, letzter Login)
4. Vom Benutzer eingestellte Profildaten (z.B. Adresse, Telefonnummer)
5. Bei Lehrkräften, vom Benutzer erzeugte Inhaltsdaten (z.B. Notizen für Schüler*innen/ für Lehrkräfte, gebuchte Ressourcen, verschickte Nachrichten)
6. Vom Nutzer angemeldete Geräte zum Zugriff auf WebUntis und Aktivierung von 2FA

Du bekommst einen Benutzernamen und ein Passwort. Das sind Kontodaten.

Viele Daten kommen vom Schulbüro. Du hast sie dem Schulbüro bei der Anmeldung an der Schule gegeben.

Einige Daten gibst du WebUntis selbst.

Wenn du WebUntis benutzt, entstehen Daten. Du siehst sie nicht alle.

4 Quelle: https://datenschutz-schule.info/service-downloads/einwilligungen-schule-nrw/download-weitere-einwilligungen-nrw/, Version 1.0, Stand 05.2021

Wofür werden meine Daten verwendet (Zweck der Verarbeitung) und auf welcher Basis (Rechtsgrundlage) passiert dies?

- **A:** Bereitstellung eines Zugangs zu WebUntis.
- **D, E, F:** Nutzung von WebUntis durch angemeldete Nutzer.
- **B:** Verwaltung von Rechten und Rollen der Benutzer entsprechend der Funktion (Schüler / Lehrkraft / Eltern) und der Zugehörigkeit zu Klassen und Gruppen.
- **C:** Technische Bereitstellung von für die Verwaltung und Nutzung der WebUntis erforderlichen Diensten.
- **C:** Sicherheit und Funktionalität dieser Dienste.

WebUntis muss wissen, wer du bist. Es weiß dann, welche Stundenpläne du sehen darfst.

Die Verarbeitung der oben genannten personenbezogenen Daten erfolgt auf der Rechtsgrundlage von:

- **A, B:** Art. 6 Abs. 1 lit e), Abs. 3 lit b) DSGVO in Verbindung mit § 98 HmbSG – Datenverarbeitung im Schulbereich
- **C:** Art. 6 Abs. 1 lit. e), Abs. 3 lit. b) DSGVO in Verbindung mit § 98 HmbSG – Datenverarbeitung im Schulbereich
- **D, E, F:** Einwilligung (Artikel 6 Abs. 1 lit. a DSGVO) durch die Betroffenen.

WebUntis speichert deine Kontodaten,

- *solange du hier Schüler bist,*
- *solange du damit einverstanden bist.*

Werden meine Daten weitergegeben und wer hat Zugriff auf meine Daten?

Die Nutzung von WebUntis ist nur möglich, wenn man dafür von **WebUntis GmbH/ Hamburger Behörde für Schule und Berufsbildung (BSB)** bereitgestellte Dienste nutzt. Dieses sind Dienste zur Verwaltung von Nutzern und Inhalten.

Deine Daten bleiben immer bei der Schule. WebUntis darf mit deinen Daten nur machen, was deine Schule erlaubt.

Auftragsverarbeiter - nach Weisung durch die Schulleitung

- Von der Schule / vom Schulträger beauftragter Dienstleister **WebUntis GmbH/ Hamburger Behörde für Schule und Berufsbildung (BSB)**

Innerhalb der Schule wird der Zugriff auf die Daten im Zusammenhang mit der Nutzung von WebUntis durch das Rechte- und Rollenkonzept geregelt.

Die Schulleitung kann alles sehen. Das ist normal. Unser Administrator darf alles sehen. Das darf er nur, weil die Schulleitung es ihm erlaubt.

- **Schulleitungsmitglieder** - alle Daten, ohne administrative Rechte
- **Schulische Administratoren** - alle Daten aller Personen (auf Weisung der Schulleitung)
- **Lehrkräfte** - eigene Daten; alle Stunden- und Vertretungspläne einsehen
- **Schüler** - eigene Daten; eigene Stunden- und Vertretungspläne

Personen von **außerhalb der Schule** erhalten nur Zugriff auf Daten, wenn ein Gesetz es ihnen gestattet

Wenn du etwas Schlimmes angestellt hast oder es so aussieht als ob, dann darf die Polizei deine Daten ansehen. Die Schule informiert dich dann darüber.

- **Eltern** über das Konto ihrer Kinder: eigene Daten Schüler; Stunden- und Vertretungspläne des Kindes
- Eltern und (ehemalige) Schülern (Auskunftsrecht Art. 15 DS-GVO)
- Ermittlungsbehörden im Fall einer Straftat

Werden meine Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Nein. Die Server unseres Anbieters stehen in Österreich, kein Drittland nach DSGVO.

Nein.

Findet eine automatisierte Entscheidungsfindung statt?

Nein, in WebUntis wird nichts von Algorithmen entschieden, was die Benutzer in der Schule betrifft. Es werden keine Profile von Schülern oder Lehrkräften aus den in diesen Diensten verarbeiteten Daten erstellt.

Nein! In WebUntis entscheiden nur Menschen, keine Computer.

Wie lange werden meine Daten gespeichert?

Die Benutzerdaten von Schülern und Lehrkräften im Zusammenhang mit dem Zugang zu WebUntis über Browser und App (Kontodaten) werden solange gespeichert wie diese

- WebUntis nutzen,
- an der Schule Schüler oder Lehrkräfte sind,
- der Einwilligung in die Verarbeitung ihrer Daten nicht widersprochen haben
- (es gilt jeweils das zuerst Zutreffende)
- Nach Beendigung der Nutzung des Zugangs zu WebUntis, Verlassen Schule bzw. Ende des Dienstes an Schule oder Widerspruch in die Verarbeitung werden die Kontodaten des Benutzers innerhalb von sechs Wochen endgültig aus WebUntis gelöscht. **WebUntis GmbH/ Hamburger Behörde für Schule und Berufsbildung (BSB)** löscht sämtliche Daten danach von allen Servern und Sicherheitskopien in einem Zeitraum von 6 Monaten.
- Durch Lehrkräfte eingetragene Informationen in Stunden- und Vertretungsplänen werden entsprechend VO-DV I §9 bzw. VO-DV II §9 für 5 Jahre aufbewahrt.
- Daten im Zusammenhang mit der Erstellung von Verwaltung von Benutzerkonten für die Nutzung der WebUntis, die in der Schulverwaltung vorliegen, werden entsprechend VO-DV I §9 bzw. VO-DV II §9 für 5 Jahre aufbewahrt.
- Benutzer haben jederzeit die Möglichkeit, von ihnen eingestellte Kontaktdaten und Freigaben eigenständig zu löschen.

Solange du dein WebUntis Konto nutzt, speichert die Schule deine Kontodaten. Wenn du die Schule verlässt, löschen wir deine Kontodaten. Das tun wir auch, wenn du deine Einwilligung widerrufst.

Erst löschen wir die Daten. Dann löscht Webuntis die Daten auch noch einmal. Das dauert etwa 6 Monate. Danach ist alles weg.

Was du in dein Konto hineingeschrieben hast, kannst du immer auch selbst löschen.

Welche Rechte habe ich gegenüber der Schule?

Gegenüber der Schule besteht ein Recht auf **Auskunft** über Ihre personenbezogenen Daten, ferner haben Sie ein Recht auf **Berichtigung**, **Löschung** oder **Einschränkung**, ein **Widerspruchsrecht** gegen die Verarbeitung und ein Recht auf **Datenübertragbarkeit**.

Frage deine Schule, wenn du wissen willst,
welche Daten es von dir gibt,
du einen Fehler gefunden hast,
du möchtest, dass etwas gelöscht wird,
du die Verarbeitung verbieten möchtest,
du deine Daten mitnehmen möchtest an eine andere Schule.

Wo finde ich weitere Informationen zum Thema Datenschutz und WebUntis?

Weitere Informationen zum Thema Datenschutz findet man beim Anbieter Untis GmbH unter
https://www.untis.at/warum-untis/ueber-das-produkt/datenschutz-und-sicherheit

Nutzungsregelungen für WLAN-Zugang und Internet-Nutzung an unserer Schule[5]

Das Gymnasium Allermöhe eröffnet seinen Schülerinnen und Schülern im Bereich des

Schulgeländes als freiwilliges Angebot auf Antrag kostenlos den Zugang zum Intranet und Internet über ein WLAN, wenn die folgenden Regelungen anerkannt werden. Diese sind Teil der Schulordnung. Zudem ist die Nutzung ist im Schulgesetz (§98) geregelt[6].

Ein Anspruch auf Zulassung zur Internetnutzung besteht nicht. Das freiwillige Angebot der Internet-Nutzungsmöglichkeit kann individuell oder generell durch die Schule eingeschränkt werden.

Mit der Beantragung eines Zugangs sind folgende Regelungen zu beachten:

Die Regelungen gelten für private und für befristet durch die Schule zur Nutzung überlassene Geräte:

1. Der Zugang zum Internet darf nur für schulische Zwecke genutzt werden. Die Nutzung des Zugangs ist ausschließlich auf Recherche- bzw. Darstellungszwecke für schulische Zwecke begrenzt. Die gesetzlichen Vorschriften zum Jugendschutzrecht, Urheberrecht und Strafrecht sind zu beachten. Insbesondere dürfen keine Urheberrechte an Filmen, Musikstücken o.Ä. verletzt werden, z.B. durch die Nutzung von Internet-Tauschbörsen.
2. Die WLAN-Nutzung beschränkt sich auf maximal 3 technisch identifizierbare Geräte (MAC-Adressen) pro Schülerin oder Schüler.
3. Der Zugang zum WLAN ist nur personenbezogen in Kombination von MAC-Adresse des eingesetzten Gerätes und zugehörigem Passwort bzw. mit Hilfe des IServ-Benutzerkontos möglich. Es ist untersagt, diese Daten Dritten zugänglich zu machen; im Zweifelsfall haftet der registrierte Nutzer/die registrierte Nutzerin für unzulässige Aktivitäten Dritter bei der Nutzung seines/ ihres WLAN-Zugangs.
4. Nutzungseinschränkungen durch das Vorhandensein von Jugendschutzfiltersoftware der Schule sind zu akzeptieren. Der Versuch, die technischen Filtersperren zu umgehen, kann zum Entzug der Nutzungserlaubnis führen.
5. Die Schule übernimmt keine Haftung für die Datensicherheit der von den Schülerinnen und Schülern genutzten privaten Geräte. Die Verantwortung hierfür liegt ausschließlich bei den Nutzerinnen und Nutzern.
6. Manipulationsversuch an der Netzinfrastruktur können zivil- und strafrechtlich verfolgt werden.
7. Die Nutzungsaktivitäten der Schülerinnen und Schüler werden personenbezogen protokolliert und gespeichert[7]. Diese können im Fall der missbräuchlichen Nutzung des Zugangs[8] von der Schule oder einem von ihr beauftragten Dienstleister ausgewertet oder personenbezogen an Strafverfolgungsbehörden übermittelt werden.
8. Wenn im Verdachtsfall die gespeicherten Protokolldaten ausgewertet werden, dann erfolgt die Auswertung durch die von der Schulleitung schriftlich bestimmten Personen. Dabei wird das Vier-Augen-Prinzip eingehalten. Die Auswertung der Protokolldaten wird schriftlich dokumentiert.

Der Widerruf der Einwilligungserklärung kann ohne die Angabe von Gründen jederzeit erfolgen.

5 Quelle: https://iserv.de/downloads/privacy/
6 Hamburger Schulgesetz: https://www.hamburg.de/contentblob/1995414/5b23ded37092b4e61d0716878dba9bae/data/schulgesetzdownload.pdf S. 102ff.

Moodle Nutzungsbedingungen[9]

Herzlich willkommen auf der Lernplattform des Gymnasium Allermöhe! (Kurz: Moodle GymAll) Bevor Sie Moodle GymAll nutzen, lesen Sie bitte die folgende Datenschutzerklärung. Bei Fragen dazu wenden Sie sich bitte an die Administration unter der E-Mail Adresse thies.henken@gymall.de.

1. Teilnehmer

Wer an Moodlekursen, die zur Begleitung und Ergänzung von Präsenzveranstaltungen eingesetzt werden, teilnehmen möchte, muss sich registrieren. Die Registrierung kann nur über eine Schuladresse des Gymnasium Allermöhe (Vorname.Nachname@gymall.de) oder der Schulbehörde Hamburg (Eduport, BSB) erfolgen. Falls Sie sich mit einer anderen Adresse registrieren möchten, kontaktieren Sie bitte die Adminstration - das sind derzeit Herr Henken und Herr Lee.

Für den Fall, dass der/die Nutzer/in minderjährig ist, ist eine Registrierung nur mit Zustimmung der Eltern/Erziehungsberechtigten gestattet. Diese muss schriftlich der betreuenden Lehrkraft vorliegen.

Sobald Sie sich registrieren oder die Seite anderweitig nutzen, übermitteln Sie an Moodle Daten, die von der Plattform verarbeitet und möglicherweise auch gespeichert werden. Dies ist zum Beispiel die IP-Adresse, der Nutzername (sofern Sie eingeloggt sind), die Nutzungsuhrzeit und ähnliches. Es handelt sich hierbei teilweise um personenbezogene Daten. Darum gilt auch für uns die Datenschutzgrundverordnung der EU und das Datenschutzgesetz der Bundesregierung Deutschland. Unserer Informationspflicht über Art und Umfang der Erhebung von personenbezogenen Daten und Art und Weise ihrer weiteren Verarbeitung kommen wir mit diesem Schreiben nach, für weitere Details kontaktieren Sie bitte die Administration.

Als registrierter Nutzer können Sie die Daten, die Moodle GymAll über sie speichert, in ihrem persönlichen Nutzerprofil einsehen. Sie können Ihre Profildaten editieren und um freiwillige Angaben ergänzen. Bitte denken Sie stets daran, dass die Profilangaben für alle Nutzer der Plattform einsehbar sind. Ihre Emailadresse wird standardmäßig allen Nutzern angezeigt, die im selben Kurs eingeschrieben sind.

Sie sind verpflichtet, Ihre Zugangsdaten geheim zu halten und nicht an Dritte weiterzugeben. Sie haften für jeglichen Missbrauch ihres jeweiligen Accounts, der aufgrund ihres Verschuldens entsteht.

Wenn Moodle GymAll ohne Registrierung genutzt wird, erfolgt ein Login als Gast. Auch hierbei wird die IP-Adresse aus technischen Gründen erhoben. Sie können ausschließlich vom Administrator und nur zu Support-Zwecken eingesehen werden, siehe Punkt 12 der Datenschutzhinweise.

2. Kurse

Kurse werden von Lehrkräften erstellt und können zugangsbeschränkt sein. Die Zugangsschlüssel zu den Kursen geben allein die Lehrkräfte in den zugehörigen Präzensveranstaltungen aus. Im Missbrauchsfalle können die Zugangsschlüssel geändert werden. Die Weitergabe von Zugangsdaten jedweder Art in Social-Media-Plattformen oder via unverschlüsseltem Mailverkehr ist untersagt. Die Rolle eines/einer Lehrkraft können nur Lehrkräfte erhalten, die auf die Datenschutzrichtlinien verpflichtet wurden und der Administration persönlich bekannt sind.

Sie können sich jederzeit aus einem Kursraum als Nutzer/in wieder austragen. Falls die Kursteilnahme von Ihrer Lehrkraft als verpflichtend vorgegeben wurde, wird ein selbstständiges Austragen dieselben Konsequenzen wie ein unentschuldiges Fehlen nach sich ziehen können.

3. Urheberrechten und anderen gesetzlichen Vorgaben - Pflichten des Nutzers/der Nutzerin

Sie sind zur Einhaltung der Gesetze, insbesondere zur Wahrung von Persönlichkeits-, Urheber-, Leistungs- und Markenschutzrechten verpflichtet. Es ist darüber hinaus nicht gestattet, die Lernplattform für Werbe- und Marketingbotschaften zu verwenden. Sie sind verantwortlich für die Materialien, die Sie in das Moodle hochladen oder anderweitig einbringen (Feeds, Links, Material, Chatbeiträge usw.).

7 Die entsprechenden Vorgaben der zuständigen Datenschutz-Aufsichtsbehörde sind für die Schule bindend,
8 im Rahmen von Ermittlungsverfahren ist die Schule ggfs. verpflichtet, diese Daten den Ermittlungsbehörden zur Verfügung zu stellen.
9 Quelle: https://moodle-ola.de/moodle-datenschutz.html

Beachten Sie dabei stets das geltende Urheberrecht. Sie sind auch verpflichtet, das Urheberrecht der in Moodle erstellten Inhalte der anderen Nutzerinnen und Nutzer zu wahren. Die Betreiberin wird von Ansprüchen Dritter in diesem Zusammenhang freigestellt, Ansprüche werden an Sie weitergeleitet werden. Ausgenommen ist die unvermeidliche Herstellung automatischer temporärer Kopien durch den verwendeten Browser, das Ausdrucken von Inhalten zu privaten Lernzwecken und Materialien unter freien Lizenzen.

Straftaten, Ordnunungswidrigkeiten, insbesondere rassistische, diskriminierende oder gewalttätige Aussagen, und andere, den Lernkontext störende Handlungen sind verboten, insbesondere Beleidigungen, Verleumdungen und Bedrohung. Sie haben sich stets an die Jugendschutzvorschriften zu halten. Beachten Sie insbesondere, dass es sich bei dieser Lernplattform um eine Plattform handelt, auf der auch Minderjährige aktiv sind.

Sie verpflichten sich darüber hinaus, keine Anwendungen auszuführen, die zu einer Veränderung der Datenstruktur von Moodle führen können.

Datenschutzhinweise

1. Freiwilligkeit

Die Benutzung von Moodle ist Ihnen grundsätzlich freigestellt. Verpflichtungen zur Nutzung sind mit der entsprechenden Lehrkraft zu klären.

2. Verarbeitung personenbezogener Daten

Es werden von Moodle GymAll die nachfolgend genannten personenbezogenen Daten verarbeitet: Bei jedem Betreten und Nutzen der Webseite werden die IP-Adresse und die besuchten Seitenelemente verarbeitet und gespeichert. Dies ist nötig, um den Dienst zur Verfügung zu stellen und warten zu können. Alle Log-Daten werden nach einem Halbjahr (30 Wochen) automatisch gelöscht. Die Dauer der Speicherung resultiert aus der im deutschen Schulsystem üblichen Bewertungszyklen, für die eine Prüfung von Aussagen zur Teilnahme an Kurselementen notwendig sein könnte und daher möglich sein muss. Bei Ihrer Registrierung in Moodle werden Ihr Nachname, Ihr Vorname sowie Ihre E-Mail-Adresse in die Moodle-Datenbank übertragen. Vor- und Nachname dürfen dabei keine Pseudonyme sein, um den reibungslosen Schulablauf auch im digitalen Raum zu gewährleisten. In ihrem jeweiligen persönlichen Profil können Sie Personenbeschreibung, Bild und weitere Daten freiwillig angeben. Ihre Rolle (Lehrer/in oder Schüler/in) sowie die oben genannten Daten können von Lehrkräften und anderen Teilnehmer/innen eingesehen werden. Die Sichtbarkeit der E-Mail-Adresse im Nutzerprofil für andere Nutzerinnen & Nutzer kann eingestellt werden: sie kann ausgeblendet werden, nur für Teilnehmer/innen der von Ihnen belegten Kurse oder für alle Nutzerinnen & Nutzer sichtbar sein. Für Administratoren und Dozierende ist Ihre E-Mail-Adresse im Nutzerprofil immer sichtbar. Ebenso werden Angaben zu Land und möglicher Webseite durch Moodle systemseitig abgefragt. Diese Angaben sind alle freiwillig. Das Gymnasium Allermöhe teilt diese personenbezogenen Daten nicht mit Dritten - davon ausgenommen sind die Daten, die gemäß Vertrag an den Provider Contabo übermittelt werden müssen, um den Dienst bereitstellen zu können. Kurse und Kursinhalte dürfen nicht veröffentlicht werden, es sei denn, es handelt sich um einen öffentlich zugänglichen Kurs oder es liegt eine ausdrückliche Erlaubnis des Nutzers/der Nutzerin vor, der bzw. die diesen Inhalt verfasst hat. Werden Kurse und Kursinhalte erneut verwendet, müssen beim Export alle Nutzerdaten entfernt werden.

3. Chat

Der Chat ermöglicht eine Kommunikation in Echtzeit. Nachrichten, die Sie im Chat einbringen, sind mit dem Tag und der Uhrzeit des Beitrags, Ihrem Namen und soweit Ihr Profil ein Bild enthält auch mit diesem für alle Kursteilnehmer/innen sichtbar. Chatsitzungen werden als Protokoll gespeichert und können vom Kursbetreuer und der Administration eingesehen werden. Es obliegt der Lehrkraft, hier eine angemessene Löschungsfrist einzustellen.

4. Foren

In Foren können Sie zeitversetzt mit anderen Kursteilnehmern und Teilnehmerinnen kommunizieren. Die Beiträge sind mit Datum und Uhrzeit des Beitrags, Ihrem Namen und soweit Ihr Profil ein Bild enthält auch mit diesem für alle Kurteilnehmerinnen & Kursteilnehmer sichtbar. Beiträge, die Sie z. B. innerhalb

von Foren verfassen, sind auch zu einem späteren Zeitpunkt, wenn Sie nicht mehr als Nutzer/in aktiv sind, verfügbar. Diese Beiträge sind vergleichbar mit Leserbriefen in einer Zeitung. Nach der Veröffentlichung kann man diese auch Jahre später noch nachlesen, sofern der Kurs nicht gelöscht wurde.

5. Mitteilungen

Wenn Sie sich als Nutzer/in in Kurse eintragen, erhalten Sie aus diesen Kursräumen Nachrichten per E-Mail. In Ihrem persönlichen Profil können Sie dazu die Einstellungen anpassen. (z. B. Einzel-E-Mails oder tägliche Zusammenfassungen der von Ihnen abonnierten Foren) Lehrkräften steht in ihren Kursen und Arbeitsgruppen eine Liste der Teilnehmer/innen für Sammelmitteilungen zur Verfügung.

6. Glossar und Wiki

Beiträge im Glossar und im Wiki sind mit dem Tag, der Uhrzeit des Beitrags, Ihrem Namen und soweit Ihr Profil ein Bild enthält auch mit diesem versehen und für die anderen Moodle- Nutzerinnen & Nutzer sichtbar. In öffentlichen Kursen schließt dies auch alle Gastzugänge mit ein. Beiträge in Wiki-Aktivitäten in offenen Kursen unterliegen der offenen Lizenz CC-BY SA 4.0 International unterliegen und können als solche von anderen Personen in und außerhalb des Moodles geteilt, bearbeitet und verwendet werden. Beachten Sie hierzu die Ansage der betreuenden Lehrkraft im Kurs.

7. Logdaten

Über die in der Anmeldung selbst angeforderten o. g. Informationen hinaus protokolliert die zugrunde liegende Software Moodle, zu welcher Zeit welche Nutzerinnen & Nutzer auf welche Bestandteile der Seite und auf welche Profile anderer Nutzerinnen & Nutzer zugreifen. Protokolliert wird ferner je nach Ausgestaltung des einzelnen Angebots, ob Sie gestellte Aufgaben erledigt, ob und welche Beiträge Sie in den eventuell angebotenen Foren geleistet und ob und wie sie in Workshops oder Tests mitgewirkt haben. Die Logdaten sieht jede/r Teilnehmer/in bezüglich seiner/ihrer eigenen Daten. Lehrkräfte haben Zugriff auf Testergebnisse und andere Rückmeldungen aus den angebotenen Aktivitäten. Logdaten werden gelöscht, wenn der Kurs gelöscht wird. Dies obliegt der Verantwortung der betreuenden Lehrkraft.

8. RSS-Feeds u.a.

Externe Informationen können nicht nur durch Links/Verweise auf Drittsysteme kenntlich und aktiv nutzbar gemacht werden, sondern auch beispielsweise als Bilddatei, IFrame o. Ä. aus anderen Webangeboten (z.B. RSS-Feeds) direkt in eine Moodle-Seite eingebunden sein. In diesem Fall übermittelt Ihr Browser auch an das Drittsystem Daten.

9. Löschung von Daten

Die Registration wird nach Ablauf von 52 Wochen Inaktivität ausgesetzt, der Account wird anschließend mit einer Warndauer von 60 Tagen automatisch gelöscht. Wünschen Sie eine raschere Löschung, können Sie dies jederzeit per Mail bei der Administration beantragen. Sie werden über beide Prozesse per Mail informiert. Profildaten, die Sie zur Gestaltung Ihres Profils freiwillig eingegeben haben, können Sie jederzeit selbst löschen. Die Löschung eines Kurses kann jederzeit durch die Lehrenden veranlasst werden. Damit werden auch die Beiträge der Lernenden innerhalb des Kurses gelöscht. Beiträge und Kommentare in Foren, Wikis und im Glossar sowie von bereit gestellten Dateien sind auch nach der Deaktivierung Ihres Moodle-Zugangs für andere Nutzerinnen & Nutzer abrufbar, bis der entsprechende Kurs oder die entsprechenden Aktivitäten gelöscht wird. Logdaten werden nach einem Halbjahr (30 Wochen) dauerhaft gelöscht. (Zuvor bleiben sie erhalten, um eventuelle Nachfragen zu Bewertungen beantworten zu können.)

10. Datensicherheit

Die Kommunikation mit Moodle GymAll erfolgt über eine verschlüsselte und authentifizierte Verbindung. Die Kursräume sind vor der Indizierung durch Suchmaschinen geschützt. Zur eventuell erforderlichen Wiederherstellung des Systems wird ein Backup mit einer festen Aufbewahrungszeit erstellt. Der Serverstandort ist in der EU, der Serverbetreiber contabo.com. Der Server wird gemietet von dem Gymnasium Allermöhe. Contabo.com speichert Ihre IP 7 Tage, alle anderen Serverlogs 4 Wochen. Grundlage

hierfür ist DSGVO §6 Absatz b und c - es ist notwendig, um die Serverdienstleistung anbieten und warten zu können und entspricht den gesetzlichen Aufbewahrungspflichten.

11.Cookies

Moodle GymAll speichert in Ihrem Browser temporär einen Cookie, der Ihren Log-In-Status verwaltet. Dies muss zugelassen werden, da Sie sich sonst für jede Handlung erneut anmelden müssten. Der Cookie wird mit Beendigung der Browsersession gelöscht.

12. Administration

Administratoren haben Zugang zu allen in der Lernplattform entstehenden Daten. Sie dürfen davon nur im eng begrenzten Rahmen ihrer Aufgaben Gebrauch machen. Im Administrationsprozess werden keine personenbezogenen Daten an Dritte weitergeben, auch nicht in anonymisierter Form. Gesetzliche Übermittlungspflichten bleiben davon unberührt.

13. Auskunfts- und Berichtigungsrecht

Nach dem deutschen Datenschutzgesetz haben Sie das Recht, Auskunft über die zu Ihrer Person gespeicherten Daten zu beantragen und/oder unrichtig gespeicherte Daten berichtigen zu lassen. Wenden Sie sich hierzu bitte an die Administration.

14. Haftungsausschluss

Das Gymnasium Allermöhe ist Diensteanbieter der Lernplattform im Sinne des § 10 Telemediengesetz. Das Bereitsstellen der Plattform erfolgt nach dem Hamburger Schulgesetz, $98b. Der Betreiber ist danach für die fremden Informationen, die Sie in Moodle übermitteln oder zu denen Sie Zugang zur Nutzung in Moodle gewähren, grundsätzlich nicht verantwortlich. Etwas anderes gilt nur dann, wenn der Betreiber als Dienstanbieter Kenntnis von den rechtswidrigen Handlungen oder Informationen erhält und nicht unverzüglich tätig wird, um diese Informationen zu entfernen oder den Zugang zu ihnen sperren, sobald Sie Kenntnis erlangt haben. Der Betreiber macht sich darüber hinaus Inhalt, der innerhalb seines Angebots per Hyperlinks durch Nutzende von Moodle zugänglich gemachten fremden Websites ausdrücklich nicht zu eigen und kann deshalb für deren inhaltliche Korrektheit, Vollständigkeit und Verfügbarkeit keine Gewähr leisten. Für rechtswidrige Inhalte der hinter den Hyperlinks befindlichen Internetseiten haftet der Betreiber ebenfalls nicht.

Einwilligungserklärung

Mit der Registrierung und Nutzung von https://moodle.gymall.de geben Sie in Kenntnis der obenstehenden Nutzungsbedingungen und Datenschutzhinweise Ihre Einwilligung zu der bezeichneten Datenerhebung und -verwendung. Diese Einwilligung können Sie jederzeit widerrufen. Damit wird Ihr Nutzungszugang gelöscht. Schreiben Sie dazu eine E-Mail an: thies.henken@gymall.de oder wenden Sie sich an Herrn Henken

Bring your own Device (BYOD): Nutzungsordnung und Haftungsausschluss

Diese Nutzungsordnung regelt die Nutzung privater Schülerendgeräte am Gymnasium Allermöhe. Die Vereinbarungen gelten für alle Schülerinnen und Schüler, die ihre eigenen digitalen Endgeräte im Unterricht nutzen möchten. Die Nutzung erfolgt auf freiwilliger Basis und setzt die Zustimmung zur Nutzungsordnung durch Unterschrift voraus.

Geräte

1. Die Nutzung privater Schülerendgeräte im Unterricht ist gestattet, sofern die Nutzungsordnung akzeptiert wurde und die Lehrkraft BYOD erlaubt.
2. Die Schule übernimmt keine Verantwortung für den Zustand der Geräte. Die Schülerinnen und Schüler sind selbst für die Funktionalität, den Transport und eventuelle Schäden an ihren Geräten verantwortlich.
3. Die Schule stellt keinen technischen Support für private Schülerendgeräte bereit.

Internetnutzung

1. Die Nutzung des schulinternen WLAN-Netzwerkes mit privaten Endgeräten bedarf der Genehmigung durch die Lehrkräfte.
2. Die Nutzung des Schulnetzwerkes ist ausschließlich zu Recherche- und Darstellungszwecken gestattet.
3. Es ist untersagt, Internetseiten mit verbotenen Inhalten aufzurufen.
4. Die Schülerinnen und Schüler tragen die Kosten für die Nutzung eines privaten Hotspots selbst.

Nutzung im Unterricht

1. Die Nutzung privater Endgeräte im Unterricht ist nur nach Anerkennung der Nutzungsordnung und der ausdrücklichen Genehmigung der Lehrkräfte gestattet.
2. Die Nutzung erfolgt freiwillig und richtet sich nach den in dieser Nutzungsordnung festgelegten Bedingungen.
3. Die Nutzung darf Mitschüler nicht stören oder vom Unterricht ablenken.
4. Das Endgerät muss sich im "Lautlos-Modus" und im Flugmodus befinden, es sei denn, die Lehrkraft erlaubt ausdrücklich eine andere Nutzung.
5. Die Nutzung des Internets erfolgt gemäß den Regeln in Punkt „Internetnutzung“ dieser Nutzungsordnung.

Dokumentation der Unterrichtsinhalte

1. Die Mitschrift der Unterrichtsinhalte mit privaten Endgeräten ist gestattet, sofern die Lehrkraft dies erlaubt.
2. Die Organisation der digitalen Strukturen und die Speicherung der Daten liegt in der Verantwortung der Schülerinnen und Schüler. Eine strukturierte und übersichtliche Speicherung der Daten ist erforderlich.
3. Lehrkräften ist auf Aufforderung Einsicht in die betreffenden Unterlagen zu gewähren.

Medien und Multimedia

1. Multimediale Lerninhalte dürfen auf eigene Verantwortung und nach Genehmigung durch die Lehrkraft mit privaten Endgeräten geöffnet und abgespielt werden.
2. Zur Nutzung multimedialer Lerninhalte müssen Kopfhörer verwendet werden.
3. Es ist untersagt, verbotene Inhalte in den Dateien zu speichern oder aufzurufen.
4. Die Anfertigung und Speicherung von Bild-, Ton- oder Audiodateien, auf denen andere Personen zu erkennen sind, ist nicht gestattet, es sei denn, es erfolgt auf Aufforderung bzw. im Rahmen

einer Aufgabenstellung durch die Lehrkraft und mit dem Einverständnis der beteiligten Personen.

Experimente im naturwissenschaftlichen Unterricht

1. Private digitale Endgeräte dürfen auf eigene Gefahr für Experimente im naturwissenschaftlichen Unterricht verwendet werden, sofern die Lehrkraft dies gestattet.
2. Die Schule übernimmt keine Haftung für Beschädigungen an den Geräten während der Experimente.

Haftungsausschluss

Die Schule übernimmt keine Haftung für Schäden, Verlust oder Diebstahl von privaten Schülerendgeräten.

Schlussbestimmungen

Diese Nutzungsordnung tritt mit Unterzeichnung durch den Schüler bzw. die Erziehungsberechtigten in Kraft und bleibt bis auf Widerruf gültig. Die Schule behält sich das Recht vor, die Nutzungsbedingungen bei Bedarf zu erweitern oder anzupassen. Die Entscheidung, ob BYOD im Unterricht zugelassen ist, liegt im Ermessen der Lehrkraft.

Office 365[10]

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhältst du/ erhalten Sie Zugang zum pädagogischen Netz unserer Schule und zu unserer Arbeitsplattform Office 365 Education (im Folgenden „Office 365“). Den Zugang zu Office 365 stellen wir dir/Ihnen auch außerhalb des Unterrichts **zur schulischen Nutzung** Verfügung. Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, der Arbeitsplattform Office 365 sowie den eigenen personenbezogenen Daten und denen von anderen in der Schule lernenden und arbeitenden Personen voraus. Die folgende Nutzungsvereinbarung informiert und steckt den Rahmen ab für eine verantwortungsvolle Nutzung und ihre Annahme bzw. die Einwilligung sind Voraussetzung für die Erteilung eines Nutzerzugangs.

Nutzungsvereinbarung

Geltungsbereich

Die Nutzungsvereinbarung gilt für Schüler und Lehrkräfte, nachfolgend "Benutzer" genannt, welche das von der Schule bereitgestellte pädagogische Netzwerk und Office 365 zur elektronischen Datenverarbeitung nutzen.

Laufzeit

Dem Benutzer werden innerhalb seiner Dienstzeit/ Schulzeit ein Office 365 Zugang zur Verfügung gestellt. Beim Verlassen der Schule wird der Zugang gelöscht.

Datenschutz und Datensicherheit

Die Schule sorgt durch technische und organisatorische Maßnahmen für den Schutz und die Sicherheit der im pädagogischen Netz verarbeiteten personenbezogenen Daten. Mit Microsoft wurde zur Nutzung von Office 365 ein Vertrag abgeschlossen, welcher gewährleistet, dass personenbezogene Daten von Benutzern nur entsprechend der Vertragsbestimmungen verarbeitet werden.

Microsoft verpflichtet sich, die personenbezogenen Daten von Benutzern in Office 365 nicht zur Erstellung von Profilen zur Anzeige von Werbung oder Direkt Marketing zu nutzen. Ziel unserer Schule ist es, durch eine Minimierung von personenbezogenen Daten bei der Nutzung von Office 365 auf das maximal erforderliche Maß, das Recht auf informationelle Selbstbestimmung unserer Schüler und Lehrkräfte bestmöglich zu schützen.

Dieses ist nur möglich, wenn die Benutzer selbst durch verantwortungsvolles Handeln zum Schutz und zur Sicherheit ihrer personenbezogenen Daten beizutragen und auch das Recht anderer Personen an der Schule auf informationelle Selbstbestimmung respektieren.

An erster Stelle gilt dieses für die Nutzung von personenbezogenen Daten in der Cloud von Office 365. Es gilt jedoch auch für das pädagogische Netzwerk der Schule.

> Personenbezogene Daten gehören grundsätzlich **nicht** in die Microsoft Cloud, weder die eigenen noch die von anderen! Jeder Benutzer hat dafür zu sorgen, dass Sicherheit und Schutz von personenbezogenen Daten nicht durch leichtsinniges, fahrlässiges oder vorsätzliches Handeln gefährdet werden.

Verantwortungsvolles und sicheres Handeln bedeutet:

Passwörter

- müssen sicher sein und dürfen nicht erratbar sein. Sie müssen aus **mindestens 6 Zeichen** bestehen, worunter sich **eine Zahl**, **ein Großbuchstabe** und **ein Sonderzeichen** befinden müssen.

10 Quelle: https://datenschutz-schule.info/service-downloads/einwilligungen-schule-nrw/, Version 1.4, Stand 06.2021

- für Office 365 und das pädagogische Netz dürfen nicht identisch sein und auch nicht für andere Zugänge genutzt werden.

Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum pädagogischen Netz und zum persönlichen Office 365 Konto geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben werden.
- Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist der Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist ein schulischer Administrator zu informieren.
- Sollte der Benutzer in Kenntnis fremder Zugangsdaten gelangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Der Benutzer ist jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.
- Nach Ende der Unterrichtsstunde oder der Arbeitssitzung an einem schulischen Rechner bzw. Mobilgerät meldet sich der Benutzer von Office 365 und vom pädagogischen Netz ab (ausloggen).

Personenbezogene Daten

Für die Nutzung von personenbezogene Daten wie dem eigenen Name, biographischen Daten, der eigenen Anschrift, Fotos, Video und Audio, auf welchen der Benutzer selbst abgebildet ist und ähnlich gelten die Prinzipien der Datenminimierung und Datensparsamkeit.

Pädagogisches Netz

- Innerhalb des pädagogischen Netzes der Schule können, **außerhalb von Office 365**, personenbezogene Daten genutzt und gespeichert werden, solange dieses sparsam erfolgt und zu Zwecken des Unterrichts.

Office 365

- Personenbezogene Daten des Benutzers haben in Office 365 nichts verloren. Soll mit personenbezogenen Daten gearbeitet werden (z.B. Lebenslauf), muss dieses offline im pädagogischen Netz erfolgen.
- Eine Speicherung von personenbezogenen Daten in Microsoft OneDrive ist nicht zulässig.
- Die Nutzung von Office 365 ist für private Zwecke nicht zulässig.
- Bei der Nutzung von Office 365 von privaten Geräten aus, ist darauf zu achten, dass keine Synchronisation privater Daten mit OneDrive erfolgt.

E-Mail

Bestandteil des Office 365 Paketes ist auch eine schulische E-Mail Adresse, die gleichzeitig Teil der Zugangsdaten ist.

- Die Nutzung des schulischen E-Mail Kontos ist **nur für schulische Zwecke** zulässig. Eine Nutzung für private Zwecke ist nicht erlaubt.
- Wie bei den anderen Komponenten von Office 365 ist auch beim Versand von E-Mails die Nutzung von personenbezogenen Daten zu minimieren.
- Eine Weiterleitung schulischer E-Mails auf eine private E-Mail Adresse ist nicht gestattet.

Kalender

Die Aufnahme von privaten, nicht schulischen Terminen in den Kalender von Office 365 ist nicht zulässig. Dazu gehören auch die Geburtstage von anderen Benutzern aus der Schule.

- Zur Wahrung des Schutzes und der Sicherheit der eigenen personenbezogenen Daten ist es nicht zulässig, das schulische Office 365 Konto mit anderen privaten Konten von Microsoft oder anderen Anbietern zu verbinden.
- Eine Nutzung des schulischen Office 365 Kontos zur Authentifizierung an anderen Online Diensten ist nicht zulässig, außer es handelt sich um von der Schule zugelassene Dienste.

Urheberrecht

- Bei der Nutzung des pädagogischen Netzes der Schule und von Office 365 sind die geltenden Bestimmungen des Urheberrechtes zu beachten. Fremde Inhalte, deren Nutzung nicht durch freie Lizenzen wie Creative Commons, GNU oder Public Domain zulässig ist, haben ohne schriftliche Genehmigung der Urheber nichts im pädagogischen Netz oder in Office 365 zu suchen, außer ihre Nutzung erfolgt im Rahmen des Zitatrechts.
- Fremde Inhalte (Texte, Fotos, Videos, Audio und andere Materialien) dürfen nur mit der schriftlichen Genehmigung des Urhebers veröffentlicht werden. Dieses gilt auch für digitalisierte Inhalte. Dazu gehören eingescannte oder abfotografierte Texte und Bilder. Bei vorliegender Genehmigung ist bei Veröffentlichungen auf einer eigenen Website ist, der Urheber zu nennen, wenn dieser es wünscht.
- Bei der unterrichtlichen Nutzung von freien Bildungsmaterialien (Open Educational Resources - **OER**) sind die jeweiligen Lizenzen zu beachten und entstehende neue Materialien, Lernprodukte bei einer Veröffentlichung entsprechend der ursprünglichen Creative Commons Lizenzen zu lizenzieren.
- Digitalisierte Kopiervorlagen oder Inhalte aus Schulbüchern und Arbeitsheften, die von Lehrkräften im Rahmen des “Gesamtvertrag „Vervielfältigungen an Schulen““[11] im pädagogischen Netz oder in Office 365 in digitalem Format eingestellt wurden, dürfen vom Benutzer nicht an andere Personen außerhalb der Klassen- oder Kursgruppe weitergegeben werden.
- Bei von der Schule über das pädagogische Netz oder Office 365 zur Verfügung gestellten digitalen Inhalten von Lehrmittelverlagen ist das Urheberrecht zu beachten. Eine Nutzung ist nur innerhalb der schulischen Plattformen zulässig. Nur wenn die Nutzungsbedingungen der Lehrmittelverlage es gestatten, ist eine Veröffentlichung oder Weitergabe digitaler Inhalten von Lehrmittelverlagen zulässig.
- Stoßen Benutzer im pädagogischen Netz oder in Office 365 auf urheberrechtlich geschützte Materialien, sind sie verpflichtet, dieses bei einer verantwortlichen Person anzuzeigen.
- Die Urheberrechte an Inhalten, welche Benutzer eigenständig erstellt haben, bleiben durch eine Ablage oder Bereitstellung im pädagogischen Netz oder in Office 365 unberührt.

Unzulässige Inhalte und Handlungen

Benutzer sind verpflichtet, bei der Nutzung des pädagogischen Netzes und von Office 365 geltendes Recht einzuhalten.

- Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über das pädagogische Netz und Office 365 abzurufen, zu speichern oder zu verbreiten.
- Die geltenden Jugendschutzvorschriften sind zu beachten.
- Die Verbreitung und das Versenden von belästigenden, verleumderischen oder bedrohenden Inhalten ist unzulässig.
- Die E-Mail Funktion von Office 365 darf nicht für die Versendung von Massen-Nachrichten (Spam) und/oder anderen Formen unzulässiger Werbung genutzt werden.

Zuwiderhandlungen

Im Falle von Verstößen gegen diese Nutzungsordnung behält sich die Schulleitung des Gymnasium Allermöhe das Recht vor, den Zugang zu einzelnen oder allen Bereichen innerhalb des pädagogischen

11 "Schulbuchkopie." http://www.schulbuchkopie.de/. Abgerufen 11 Nov. 2020.

Netzes und von Office 365 zu sperren. Davon unberührt behält sich die Schulleitung weitere dienstrechtliche Maßnahmen (Lehrkräfte) oder Ordnungsmaßnahmen (Schüler) vor.

Nutzungsbedingungen von Microsoft für Office 365

Es gelten außerdem die Nutzungsbedingungen des Microsoft-Servicevertrags: https://www.microsoft.com/de-de/servicesagreement/ und davon soll vor allem hingewiesen werden auf den

Verhaltenskodex

Inhalte, Materialien oder Handlungen, die diese Bestimmungen verletzen, sind unzulässig. Mit Ihrer Zustimmung zu diesen Bestimmungen gehen Sie die Verpflichtung ein, sich an diese Regeln zu halten:

1. Nehmen Sie keine unrechtmäßigen Handlungen vor.
2. Unterlassen Sie Handlungen, durch die Kinder ausgenutzt werden, ihnen Schaden zugefügt oder angedroht wird.
3. Versenden Sie kein Spam. Bei Spam handelt es sich um unerwünschte bzw. unverlangte Massen-E-Mails, Beiträge, Kontaktanfragen, SMS (Textnachrichten) oder Sofortnachrichten.
4. Unterlassen Sie es, unangemessene Inhalte oder anderes Material (das z. B. Nacktdarstellungen, Brutalität, Pornografie, anstößige Sprache, Gewaltdarstellungen oder kriminelle Handlungen zum Inhalt hat) zu veröffentlichen oder über die Dienste zu teilen.
5. Unterlassen Sie Handlungen, die betrügerisch, falsch oder irreführend sind (z. B. unter Vorspiegelung falscher Tatsachen Geld fordern, sich als jemand anderes ausgeben, die Dienste manipulieren, um den Spielstand zu erhöhen oder Rankings, Bewertungen oder Kommentare zu beeinflussen).
6. Unterlassen Sie es, wissentlich Beschränkungen des Zugriffs auf bzw. der Verfügbarkeit der Dienste zu umgehen.
7. Unterlassen Sie Handlungen, die Ihnen, dem Dienst oder anderen Schaden zufügen (z. B. das Übertragen von Viren, das Belästigen anderer, das Posten terroristischer Inhalte, Hassreden oder Aufrufe zur Gewalt gegen andere).
8. Verletzen Sie keine Rechte anderer (z. B. durch die nicht autorisierte Freigabe von urheberrechtlich geschützter Musik oder von anderem urheberrechtlich geschütztem Material, den Weiterverkauf oder sonstigen Vertrieb von Bing-Karten oder Fotos).
9. Unterlassen Sie Handlungen, die die Privatsphäre von anderen verletzen.
10. Helfen Sie niemandem bei einem Verstoß gegen diese Regeln

Datenschutzrechtliche Informationen nach Art. 13 DS-GVO

Zur Nutzung unseres pädagogischen Netzes und von Office 365 an des Gymnasium Allermöhe ist die Verarbeitung von personenbezogenen Daten erforderlich. Darüber möchten wir Sie/ Euch im folgenden informieren.

Datenverarbeitende Stelle

Gymnasium Allermöhe Walter-Rothenburg-Weg 41 21035 Hamburg	Olaf Colditz olaf.colditz@bsb.hamburg.de

Zwecke der Verarbeitung personenbezogener Daten

Personenbezogene Daten der Benutzer des pädagogischen Netzes und von Office 365 werden erhoben, um dem Benutzer die genannten Dienste zur Nutzung im Unterricht und zur Vor- und Nachbereitung von Unterricht zur Verfügung zu stellen, die Sicherheit dieser Dienste und der verarbeiteten Daten aller Benutzer zu gewährleisten und im Falle von missbräuchlicher Nutzung oder der Begehung von Straftaten die Verursacher zu ermitteln und entsprechende rechtliche Schritte einzuleiten.

Rechtsgrundlage der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten bei Nutzung des pädagogischen Netzes und von Office 365 erfolgt auf der Grundlage von DS-GVO Art. 6 lit. a (Einwilligung).

Kategorien betroffener Personen

Schülerinnen und Schüler, Lehrkräfte

Kategorien von personenbezogenen Daten

Office 365

- **Anmeldeinformationen**, Rechte und Rollen, Zuteilung zu Gruppen, **Geräte- und Nutzungsdaten** (Gerätedaten nur bei BYOD und außerschulischer Nutzung relevant]**, Nutzungsdaten von Inhalten, Interaktionen, Suchvorgänge und Befehle, Text-, Eingabe- und Freihanddaten, Positionsdaten**, **Inhalte[12], Lizenzinformationen** (Anzahl Installationen, bei Nutzung von Office 365 Pro Plus)

Kategorien von Empfängern

Office 365

Intern:

- **Schulische Administratoren** (alle technischen und Daten und Kommunikationsdaten, soweit für administrative Zwecke erforderlich)
- **Schulleitung** (Zugangsdaten, alle technischen und öffentlichen Daten und Kommunikationsdaten **nur** im begründeten Verdachtsfall einer Straftat oder bei offensichtlichem Verstoß gegen die Nutzungsvereinbarung **und** nach vorheriger Information der Benutzer **und** im Beisein von Zeugen - *Vier-Augen-Prinzip*),

Extern:

- **Microsoft** (zur Bereitstellung der Dienste von Office 365, auf Weisung der Schulleitung)
- **Dienstleister, Administratoren** (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich, auf Weisung der Schulleitung)
- **Ermittlungsbehörden** (alle Daten betroffener Benutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- **US Ermittlungsbehörden** haben Zugriff nach US amerikanischem Recht (weitere Informationen, siehe unten).
- **Betroffene** (Auskunftsrecht nach Art. 15 DS-GVO)

Löschfristen

Office 365

Mit dem Ende der Schulzugehörigkeit erlischt das Anrecht auf die Nutzung von Office 365. Entsprechend wird die Zuweisung von Office 365 Education-Lizenzen zu Benutzern mit Ende der Schulzugehörigkeit, in der Regel zum Schuljahresende, aufgehoben. Damit verliert der Benutzer den Zugriff auf Online Dienste und -Daten. Das bedeutet Folgendes:

- Alle Daten im Zusammenhang mit dem Konto dieses Benutzers werden von Microsoft 30 Tage aufbewahrt. Eine Ausnahme bilden Daten mit gesetzlicher Aufbewahrungspflicht, die entsprechend dieser Fristen aufbewahrt werden.
- Nach Ablauf der 30-tägigen Frist werden die Daten von Microsoft gelöscht und können nicht wiederhergestellt werden. Ausgenommen sind Dokumente, die auf SharePoint Online-Websites gespeichert sind.[13]

12 Details siehe https://privacy.microsoft.com/de-de/privacystatement#mainenterprisedeveloperproductsmodule (soweit auf Office 365 Education zutreffend)

13 Siehe Verwalten der Lizenzen und Inhalte von Absolventen in Office 365 Education (11/2018)

Benutzer müssen ihre Daten vorher eigenständig sichern.

Recht auf Widerruf

Die erteilte Einwilligung kann für die Zukunft jederzeit widerrufen werden. Dabei kann der Widerruf auch nur auf einen Teil der der Datenarten bezogen sein. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Im Falle des Widerrufs sämtlicher Verarbeitung personenbezogener Daten im pädagogischen Netz und in Office 365 werden die entsprechenden Zugangsdaten aus dem System gelöscht und der Zugang gesperrt.

Weitere Betroffenenrechte

Gegenüber der Schule besteht ein Recht auf **Auskunft** über Ihre personenbezogenen Daten, ferner haben Sie ein Recht auf **Berichtigung**, **Löschung** oder **Einschränkung**, ein **Widerspruchsrecht** gegen die Verarbeitung und ein Recht auf **Datenübertragbarkeit**. Zudem steht Ihnen ein **Beschwerderecht** bei der Datenschutzaufsichtsbehörde, der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein Westfalen zu.

Wichtiger Hinweis - Freiwilligkeit

Wir möchten darauf hinweisen, dass sowohl die Nutzung des pädagogischen Netzes wie auch von Office 365 auf freiwilliger Basis erfolgen. Eine Anerkennung der Nutzervereinbarungen und eine Einwilligung in die Verarbeitung der zur Nutzung des pädagogischen Netzes wie auch von Office 365 erforderlichen personenbezogenen Daten ist freiwillig.

- Die Nutzung des pädagogischen Netzes setzt keine Nutzung von Office 365 voraus. Wer die Nutzungsvereinbarung für Office 365 nicht anerkennen möchte, erfährt daraus keinen Nachteil und kann mit einer Offline Version von Microsoft Office arbeiten.
- Die Nutzung von Office 365 setzt keine Nutzung des pädagogischen Netzes voraus. Alternativ ist es auch möglich, mit Einwilligung der Eltern über einen eigenen mobilen Zugang mit dem eigenen Gerät auf Office 365 zuzugreifen. Für eine brauchbare und zuverlässige Leistung einer Mobilfunkverbindung in allen Gebäudeteilen übernimmt die Schule keine Verantwortung.
- Wer die Nutzungsvereinbarung des pädagogischen Netzes nicht anerkennt, kann keine schulischen Computer und Mobilgeräte nutzen. Die Lehrkräfte werden dann anderweitig Materialien für Arbeitsaufträge im Unterricht bereitstellen. Unsere Schulbibliothek steht unseren Schülern für Recherchen jederzeit offen.
- Die Nutzung des pädagogischen Netzes setzt immer die Anerkennung der Nutzervereinbarung für das pädagogische Netz **und** die Einwilligung in die diesbezügliche Verarbeitung von personenbezogenen Daten des Betroffenen voraus.
- Die Nutzung von Office 365 setzt immer die Anerkennung der Nutzervereinbarung für Office 365 **und** die Einwilligung in die diesbezügliche Verarbeitung von personenbezogenen Daten des Betroffenen voraus.

Zusätzliche Informationen

Datenschutz bei Verarbeitung von personenbezogenen Daten in den USA

Bei der Nutzung von Office 365 können auch Daten auf Servern in den USA verarbeitet werden. Dabei geht es weniger um Inhalte von Chats, Videokonferenzen, Terminen und gestellten Aufgaben, Nutzerkonten und Teamzugehörigkeiten, sondern um Daten, welche dazu dienen, die Sicherheit und Funktion der Plattform zu gewährleisten und zu verbessern. Nach der aktuellen Rechtslage in den USA haben US Ermittlungsbehörden nahezu ungehinderten Zugriff auf alle Daten auf Servern in den USA. Nutzer erfahren davon nichts und haben auch keine rechtlichen Möglichkeiten, sich dagegen zu wehren. Die Risiken, welche durch diese Zugriffsmöglichkeiten von US Ermittlungsbehörden entstehen, dürften eher gering sein.

Thema CLOUD-Act

Im Rahmen des CLOUD-Act haben US Ermittlungsbehörden auch Möglichkeiten, bei Microsoft die Herausgabe von personenbezogenen Daten, die auf Servern in der EU gespeichert sind, zu verlagen. Dort werden die meisten Daten gespeichert, die bei einer Nutzung von Microsoft/ Office 365 und Teams anfallen. Nach Angaben von Microsoft ist die Anzahl dieser Anfragen recht gering, zudem kann Microsoft dagegen vor Gericht gehen. Die wenigsten Anfragen dürften, falls überhaupt, schulische Konten betreffen. Microsoft gibt für Juli - Dezember 2019 insgesamt 3.310 Anfragen von Ermittlungsbehörden an. Davon kamen die meisten aus Deutschland.

Wo werden meine personenbezogenen Daten verarbeitet?

Die Verarbeitung von personenbezogenen Daten in Office 365 und angebundenen Produkten erfolgt überwiegend auf Servern mit Standort Deutschland. Es ist möglich, dass sogenannte Telemetriedaten, eine Art Diagnosedaten, in den USA verarbeitet werden.

Wie sicher ist Office 365?

Die Plattform genügt allen gängigen Sicherheitsstandards für Cloud Plattformen.

Wo kann ich mehr zum Datenschutz von Office 365 erfahren?

Thema Datenschutz & Sicherheit bei Microsoft - https://www.microsoft.com/de-de/trust-center/privacy

Die aktuelle Datenschutzerklärung von Microsoft kann hier eingesehen werden:

https://privacy.microsoft.com/de-de/privacystatement

Von besonderer Bedeutung ist dabei bezüglich der personenbezogenen Daten von Personen in der Schule der folgende Abschnitt:

“Für Microsoft-Produkte, die von Ihrer K-12-Schule bereitgestellt werden, einschließlich Microsoft 365 Education, wird Microsoft:

- neben den für autorisierte Bildungs- oder Schulzwecke erforderlichen Daten keine personenbezogenen Daten von Schülern/Studenten erfassen oder verwenden,
- personenbezogene Daten von Schülern/Studenten weder verkaufen noch verleihen,
- personenbezogene Daten von Schülern/Studenten weder zu Werbezwecken noch zu ähnlichen kommerziellen Zwecken wie Behavioral Targeting von Werbung für Schüler/Studenten verwenden oder freigegeben,
- kein persönliches Profil eines Schülers/Studenten erstellen, es sei denn, dies dient der Unterstützung autorisierter Bildungs- oder Schulzwecke oder ist von den Eltern, Erziehungsberechtigten oder Schülern/Studenten im angemessenen Alter genehmigt, und
- seine Anbieter, an die personenbezogene Daten von Schülern/Studenten ggf. zur Erbringung der Bildungsdienstleistung weitergegeben werden, dazu verpflichten, dieselben Verpflichtungen für personenbezogene Daten der Schüler/Studenten zu erfüllen.”

Was tut die Schule zum Schutz meiner personenbezogenen Daten in Office 365?

Als Schule hat für uns der Schutz der personenbezogenen Daten unserer Schüler und Lehrkräfte oberste Priorität. Deshalb sorgen wir durch technische und organisatorische Maßnahmen dafür, dass die Nutzung von Office 365 mit der größtmöglichen Sicherheit abläuft. Wir haben Office 365 so voreingestellt, dass durch das Handeln und Fehler der Nutzer selbst möglichst wenige Risiken entstehen können. Ganz zentral ist die Schulung der Nutzer für einen sicheren und verantwortungsvollen Umgang mit den Werkzeugen in Office 365. Vor Erteilung des Zugangs findet eine Grundschulung statt. Diese wird durch eine jährliche Belehrung und die Nutzungsvereinbarung/ Dienstanweisung ergänzt.

Kann eine Einwilligung nach dem Urteil des EUGH zum EU-US Privacy Shield noch genutzt werden?

Das ist möglich, setzt aber voraus, dass die etwaige Übermittlung von personenbezogenen Daten in die USA entsprechend so abgesichert ist, dass sie den Vorgaben der DS-GVO entspricht. Dieses könnte beispielsweise durch zusätzliche technische Maßnahmen und Garantien Seitens Microsoft erfolgen. Die Standardvertragsklauseln, auf welche Microsoft seine Datenübermittlungen aktuell stützt, reichen nach Auffassung des EUGH alleine dafür nicht aus. Jede Schule, jeder Schulträger, jedes Bundesland hat darüber hinaus die Möglichkeit, mit Microsoft in Form von Nebenabreden in Ergänzung zu den OST und Data Processing Addendum zusätzliche Maßnahmen und Garantien auszuhandeln.

Ist es nicht möglich, die Übermittlung von personenbezogenen Daten durch zusätzliche technische Maßnahmen abzusichern, sehen viele Fachjuristen Zweifel, diese Übermittlung durch eine Einwilligung zu legitimieren, da Art. 49 Abs. 1 lit. a gemäß Art. 49 Abs. 3 ausdrücklich nicht durch öffentliche Stellen in Ausübung hoheitlicher Tätigkeiten genutzt werden kann. Das letzte Wort ist aber hier noch nicht gesprochen.

Was kann ich als Nutzer zusätzlich tun, um den Schutz meiner personenbezogenen Daten zu erhöhen?

Wenn man von einem privaten Endgerät auf Office 365 zugreift, könnte man:

- einen sicheren Browser (Brave, Firefox oder DuckDuckGo auf Mobilgeräten) nutzen, der die Erhebung zusätzlicher Daten einschränkt,
- in Browsern keine Cookies speichern bzw. die absolut erforderlichen nach Ende eine Sitzung automatisch löschen,
- den Zugang nicht über die mobilen Apps, sondern einen sicheren Browser vorzunehmen
- den Zugang über ein VPN laufen lassen, um IP und Geolocation zu verschleiern,
- den Zugang auf ein einziges System/ Gerät beschränken,
- den Zugang mit einem speziellen Nutzerkonto auf dem Rechner vorzunehmen, in dem es keine Anmeldungen an anderen Konten wie YouTube, WhatsApp, Instagram, ... gibt.
- den Zugang über eine virtuelle Maschine oder ein System von einer Live DVD/ Live Boot Stick vorzunehmen.
- wenn der Zugang über ein iPad erfolgen soll, sollte dort kein vorheriger oder gleichzeitiger Login an einer anderen nicht schulischen App oder Web-Plattform erfolgen

Ein Teil dieser Maßnahmen führt zu Komfortverlusten bei der Nutzung. Ob man einige oder mehrere dieser Maßnahmen umsetzen möchte, muss jeder Nutzer für sich entscheiden.

Datenschutzrechtliche Information zum IServ Videokonferenztool (Art. 12 DS-GVO)[14]

Auf dieser Seite informieren wir Sie aufgrund Art. 12 DSGVO über die zur Nutzung des IServ Videokonferenztools erforderliche Verarbeitung von personenbezogenen Daten.

Wer ist verantwortlich für die Verarbeitung der Daten meines Kindes?

Verantwortlich ist die Schule: Gymnasium Allermöhe, Walter-Rothenburg-Weg 41, 21035 Hamburg; Schulleitung: Olaf Colditz

An wen kann ich mich wenden, wenn ich Fragen zum Datenschutz habe?

Fragen zum Datenschutz können Sie an den behördlich bestellten schulischen Datenschutzbeauftragten stellen: Olaf Colditz, olaf.colditz@bsb.hamburg.de

Zu welchem Zweck sollen die Daten meines Kindes verarbeitet werden?

Das IServ Videokonferenztool ermöglicht Unterricht und Besprechungen, bei denen Beteiligte nicht zusammen in einem physikalischen Raum sind. Durchführung von Online-Unterrichtseinheiten in der Lerngruppe und individueller Betreuung und Beratung in Kleingruppen oder Einzeltreffen zwischen Schüler und Lehrkraft sind dadurch möglich. Zudem werden die Schüler so datenschutzkonform an das Medium und die Möglichkeiten herangeführt, die heutzutage nicht mehr wegzudenken sind.

Auf welcher Rechtsgrundlage erfolgt die Verarbeitung?

Die Verarbeitung erfolgt auf der Grundlage Ihrer Einwilligung, da IServ kein durch die Behörden genehmigtes Lehrmittel ist, ist nur diese Möglichkeit gegeben.

Welche personenbezogenen Daten meines Kindes werden bei Teilnahme an einer IServ Videokonferenz verarbeitet?

Videokonferenzen in der Schule finden in der Regel in einer Gruppe von Teilnehmern mit IServ-Account statt.

Bei der Teilnahme an einer Videokonferenz) werden neben Bild- und Tondaten zusätzliche Daten zur Konferenz verarbeitet: Name des Raumes, IP Nummer des Teilnehmers und Informationen zum genutzten Endgerät. Je nach Nutzung der Funktionen in einer Videokonferenz fallen personenbezogen Inhalte von Chats, gesetztem Status, Eingaben bei Umfragen, Beiträge zum geteilten Whiteboard, durch Upload geteilte Dateien und Inhalte von Bildschirmfreigaben an. Eine Speicherung von Videokonferenzen und den genannten Daten durch die Schule oder IServ erfolgt nicht. Es muss zum Videokonferenztool eine Nutzerordnung und Hinweise geben, da ja der Kontakt oft aus dem häuslichen Bereich der Teilnehmer erfolgt und besonders dort Daten geschützt werden sollten. Aufnahmen sind generell zu untersagen.

Wer hat Zugriff auf die personenbezogenen Daten meines Kindes?

Alle Teilnehmer einer Videokonferenz können dort Daten durch Sehen, Hören und Lesen verarbeiten. Der Präsentator hat zusätzlich die Auswertungen zu Umfragen zur Verfügung. IServ selbst hat nur Zugriff auf die Daten im Rahmen der Auftragsverarbeitung also nur auf Weisung der Schule.

An wen werden die Daten meines Kindes übermittelt und wie lange werden diese Daten gespeichert?

Unsere Videokonferenz-Instanz wird von IServ für uns betrieben. IServ verarbeitet die personenbezogenen Daten Ihres Kindes ausschließlich in unserem Auftrag. Demnach darf IServ sie nur entsprechend unserer Weisungen und für unsere Zwecke und nicht für eigene Zwecke nutzen. Es werden also keine Daten an Dritte weitergegeben. Die Daten werden bei IServ nicht gespeichert.

Die Schule speichert ebenso keine personenbezogenen Daten. Videokonferenzen und Chats werden generell nicht aufgezeichnet. Die Inhalte von Chats, geteilte Dateien und Whiteboards werden in der Platt-

14 Quelle: https://iserv.de/downloads/privacy/, Version 1.2, Stand 07.2021

form gelöscht, sobald ein Konferenzraum geschlossen wird. Ausnahmen müssen extra in der Schule vereinbart werden.

An die Server der IServ GmbH werden Klarnamen der Teilnehmer, IP-Adressen, Browserkennungen, Berechtigungen, Videokonferenz-Raum-Einstellungen, Raumname und die IP-Adresse sowie eine eindeutige Identifikationsnummer des IServs übermittelt. Auf dem Videokonferenz-Server haben die Benutzer die Möglichkeit, Daten in Form von Beteiligungen am virtuellen Whiteboard, Chat-Nachrichten, hochgeladenen Präsentationen und Notizen einzugeben. Außerdem fallen Metadaten wie Dauer der Videokonferenz und Zeitstempel zu Ereignissen wie dem Beitritt oder dem Verlassen einer Konferenz an. Diese Daten werden frühestens zum Ende der Videokonferenz und spätestens nach Ablauf von sieben Tagen gelöscht. Sicherungskopien dieser Daten werden nicht angelegt.

Technische Information: Nehmen zu viele mit aktivierter Kamera an einer Videokonferenz teil, kann es zu Stabilitätsproblemen kommen Neben der eigenen Bandbreite ist die Qualität der Konferenz auch von dem eigenen Netzwerk abhängig. Verwenden Sie möglichst eine Kabelverbindung zum Router und vermeiden Sie WLAN.

Es ist Teilnehmern untersagt, Videokonferenzen mitzuschneiden. Die Verwendung von Software, die den Bildschirminhalt oder die Videokonferenzen aufnimmt, stellt einen Verstoß gegen die DSGVO und das Recht am eigenen Bild dar. Ausnahmen müssen durch die Schulleitung genehmigt sein.

Einwilligung

Sehr geehrte Erziehungsberechtigte,

Wir legen großen Wert auf den persönlichen Kontakt zu unseren Schülerinnen und Schülern. Dazu möchten wir das Videokonferenz-Modul von IServ nutzen, um Sitzungen innerhalb der Lerngruppen unter Leitung einer Lehrkraft datenschutzkonform abhalten zu können und für Ihr Kind Beratung und Unterstützung durch Lehrkräfte in Kleingruppen und im Vier-Augen-Gespräch auch online zu ermöglichen. Das IServ Videokonferenztool, eine Plattform, die in Deutschland von vielen Schulen und Universitäten genutzt wird. Sie kann über Computer, Smartphone und Tablet genutzt werden.

Die Teilnahme an einer Videokonferenz erfordert für die Schüler nur das IServ-Nutzerkonto. Alle Inhalte der Videokonferenzen und begleitenden Chats bleiben im Kreis der Teilnehmer. Es erfolgt keine Aufzeichnung oder Speicherung durch die Schule oder den Anbieter, Aufzeichnungen durch die Teilnehmer sind durch unsere Nutzungsordnung bis auf wenige Ausnahmen untersagt. Schüler sind gehalten, bei einer Videokonferenz darauf zu achten, dass die Privatsphäre ihrer Familienmitglieder gewahrt bleibt. Bei Verstößen gegen diese Regel behält die Schule sich vor, Ihr Kind von Videokonferenzen auszuschließen bzw. die Teilnahme auf Audio zu beschränken.

Hierzu möchten wir hier Ihre Einwilligung einholen.

(O. Colditz Schulleiter)

Die Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile. Die Teilnahme ist für Ihr Kind freiwillig. Im Falle einer Nichteinwilligung werden wir Ihrem Kind auf anderen Wegen in persönlichen Kontakt treten.

Diese Einwilligung kann für die Zukunft jederzeit formlos bei der Schule widerrufen werden. Im Falle des (Teil-)Widerrufs wird Ihr Kind nicht oder nur über Ton an Videokonferenzen teilnehmen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Soweit die Einwilligung nicht widerrufen wird, gilt sie für die Dauer der Beschulung.

Gegenüber der Schule besteht ein Recht auf Auskunft über Ihre personenbezogenen Daten, ferner haben Sie ein Recht auf Berichtigung, Löschung oder Einschränkung, ein Widerspruchsrecht gegen die Verarbeitung und ein Recht auf Datenübertragbarkeit. Zudem steht Ihnen ein Beschwerderecht bei der Datenschutzaufsichtsbehörde unseres Bundeslandes zu.

Nutzungsordnung IServ Videokonferenzmodul[15]

Rahmenbedingungen

Über das Videokonferenzmodul können Webkonferenzräume in datenschutzkonformen Umgebungen zur Durchführung von synchronen Phasen des Fernlernens in Gruppen sowie zur individuellen Betreuung mit einem abgestuften Rollen- und Rechtemanagement eingerichtet und genutzt werden.

Webkonferenzen

Zugangsdaten

- An einer Webkonferenz dürfen nur berechtigte Personen teilnehmen.
- An einer Webkonferenz müssen sich die Teilnehmer mit einem persönlichen Account mit sicherem Passwort bzw. einen zeitlich befristeten, passwortgeschützten Link (Raum Sharing) anmelden.

Daten, die im Rahmen einer Webkonferenz gespeichert werden

Bei der Teilnahme an einer Videokonferenz werden folgende Daten verarbeitet:

- Nachname, Vorname
- Bild- und Audiodaten
- Name des Raumes
- IP-Nummer des Teilnehmers und Informationen zum genutzten Endgerät.
- Je nach Nutzung der Funktionen in einer Videokonferenz fallen Inhalte von Chats, gesetzter Status, Beiträge zum geteilten Whiteboard, Eingaben bei Umfragen, durch Upload geteilte Dateien und Inhalte von Bildschirmfreigaben an.

Die Aufzeichnung von Videokonferenzen ist deaktiviert.

Datenlöschung

Es werden keine personenbezogenen Daten im Zusammenhang mit der Nutzung des IServ Videokonferenz-Moduls dauerhaft gespeichert. Videokonferenzen werden nicht aufgezeichnet. Die Inhalte von Chats, Notizen, geteilte Dateien und Whiteboards werden gelöscht, sobald ein Konferenzraum geschlossen wird.

Webkonferenz: Lehrer ⇔ Schüler/in

Wird die Nutzung des Moduls von der Schule als notwendig angesehen, benötigt man keine Einwilligung der Schülerin / des Schülers bzw. der Erziehungsberechtigten.

Hinweis: Die Schülerin / der Schüler hat ein Widerspruchsrecht nach Art. 21 DSGVO, über das er in der Nutzungsordnung zu informieren ist. Die Schülerin / der Schüler ist dann auf anderen Wegen auf dem Laufenden zu halten.

Webkonferenz (Schulleitung ⇔ Lehrerkräfte; Lehrerkräfte ⇔ Lehrkräfte; Schulleitungen ⇔ Lehramtsanwärter/Lehrkräfte)

Eine Webkonferenz kann durchgeführt werden sofern sie

- *dienstlich erforderlich ist* (Konferenzen, Abteilungskonferenzen).
- Bei besonders sensiblen Meetings/Gesprächen (bspw. Einstellungsgesprächen, Beratungsgesprächen, …) ist die Leitung des Meetings in besonderer Verantwortung die Teilnahme zu schützen bzw. zu begrenzen. Geeignete Maßnahmen, wie z.B. ein Passwort-Schutz, Warteraum mit Teilnahmezulassung, akustische und optische Verifizierung der Teilnehmenden sind unabdingbar.

15 Quelle: https://iserv.de/downloads/privacy/, Version 1.2, Stand 28.06.2021

- Fortführungen von sensiblen Meetings/Gesprächen – nachdem eine teilnehmende Person das Meeting scheinbar verlassen hat -, sind in dem Bewusstsein zu führen, dass die optische nicht mehr anwesende Teilnehmende eventuell weiterhin/noch im Meeting ist. Es ist ggf. in der alleinigen Verantwortung der Organisatoren das laufende Meeting ggf. zu beenden und z.B. ein neues Meeting zu starten, um vertrauliche Gespräche zu führen.

Webkonferenz (Lehramtsanwärter ⇔ Lehramtsanwärter)

Eine Webkonferenz kann durchgeführt werden sofern die beteiligten Personen zustimmen

Regeln für Webkonferenzen und Fernunterricht

- Bei Webkonferenzen und im Fernunterricht dürfen mittels IServ Videokonferenz-Modul keine Daten nach Art. 9 Datenschutzgrundverordnung (Gesundheitsdaten, personenbezogene Daten aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit sowie Daten zum Sexualleben oder der sexuellen Orientierung hervorgehen) verarbeitet werden.
- Es ist grundsätzlich verboten, Gespräche und Übertragungen mitzuschneiden, aufzuzeichnen, zu speichern auch mit jeder Art auch mit Drittsoftware oder bspw. Handycams …, außer dass die Lehrkraft dies erlaubt.
- Es ist generell untersagt, dass ein Dritter (auch Eltern, Freunde Geschwister usw.) beim Fernunterricht zuhören zusehen oder sonst wie einen Einblick in die Kommunikation erhalten.
- Der persönliche Account für den Zugang zur Webkonferenz bzw. zum Fernunterricht darf an keine andere Person weitergegeben werden.
- Keine Nutzung in öffentlich zugänglichen Räumen wie z.B. Cafés, Kneipen, Restaurants, ÖPNV, Warteräume, Arztpraxen, Läden usw.

Hinweis: Wählen Sie einen passenden Ort für die Videokonferenz, wenn Bild- und Tonübermittlung aktiviert sind, da die anderen Konferenzteilnehmerinnen und - teilnehmer ihr privates Umfeld im Hintergrund sehen können. Ideal ist eine aufgeräumte Arbeitsumgebung mit unaufgeregtem Hintergrund oder eine weiße Wand. Kommunizieren Sie diesen Sachverhalt rechtzeitig vor der Konferenz auch an die Teilnehmenden.

Empfehlungen für die Kommunikations- und Verhaltensregeln während Webkonferenzen

- Die goldene Regel vorneweg: Wer nicht spricht, schaltet sein Mikrofon stumm! Headsets sind zwar für die Tonqualität empfehlenswert, jedoch übertragen sie auch Atem- und Schluckgeräusche besonders deutlich.
- Seien Sie sich bewusst, dass eine Kamera auf Sie gerichtet ist. Zeigen Sie eine freundliche, offene Körperhaltung und Körpersprache. Lächeln Sie!
- Schauen Sie so oft wie möglich in die Kamera. Ihre Konferenzpartner werden dies als direkte Ansprache wahrnehmen. Unter Umständen ist es hilfreich, einen Klebepunkt knapp neben der Kameralinse zu befestigen, den man mit den Augen fokussieren kann.
- Schalten Sie – wenn möglich – ihr eigenes Kamerabild klein. Die Verlockung sich selbst zu beobachten ist groß und lenkt Sie ab.
- Ändern Sie möglichst wenig an der Positionierung aus Ausrichtung der Kamera, nachdem die Konferenz begonnen hat. Nachjustierungen wirken auf die Konferenzteilnehmerinnen und –teilnehmer störend.
- Auch wenn die Webkonferenz am Computer stattfindet, vermeiden Sie „Nebenbeschäftigungen" wie Tippen auf der Tastatur oder Herumklicken in verschiedenen Fenstern – vor allem bei aktiviertem Mikrofon. Wenn Ihr Betriebssystem einen Nicht-Stören-Modus hat, schalten Sie ihn ein.
- Nutzen Sie auch den Chat nicht für Nebengespräche. Die Chats sind für Fragen und Hilfen geeignet. Schalten Sie als Lehrkraft ggf. die privaten Chats von Teilnehmerinnen und Teilnehmer ab.
- Setzen Sie klare verbale Signale für Redebeginn und Redeende. Sprechen Sie etwas langsamer und deutlicher als in der direkten Kommunikation.

- Warten Sie – z.B. nach direkten Fragen – länger auf die Reaktion von Teilnehmerinnen und Teilnehmern als bei direkten Gesprächen im „echten Leben“.
- Nutzen Sie Gestik bewusst auch für affirmative Signale beim Zuhören, wie z.B. ein deutliches Nicken oder ein Daumen-nach-oben-Zeichen.
- Bei größeren Online-Seminaren: Lassen Sie sich bei Moderationsaufgaben unterstützen um sich selbst auch besser auf die Kommunikation mit den Teilnehmerinnen und Teilnehmern konzentrieren zu können. Bestimmen Sie beispielsweise einen Moderator der die Statusicons und den Chat im Blick behält und Ihnen Wortmeldungen und Fragen zum passenden Zeitpunkt weitergibt.

Regelungen zu Videokonferenzen[16]

Videokonferenzen im Unterricht: Hinweise für die Schulgemeinschaft

Eine neue Vorschrift im Hamburgischen Schulgesetz regelt den Einsatz von Videokonferenzen im Unterricht an Hamburger Schulen. Dieser neue § 98c wurde in das Schulgesetz eingefügt, weil in der gegenwärtigen Corona-Pandemie zeitweise der Schulbetrieb auf Distanz- und Wechsel-/Hybridunterricht umgestellt werden musste.[17] Das Schulgesetz setzt den Unterricht in Videokonferenzen mit dem regulären Unterricht gleich. Das heißt es gilt auch im Unterricht über Videokonferenzen Anwesenheitspflicht. Dadurch wird zudem die Bewertung der Mitarbeit in Videokonferenzen ermöglicht.

Videokonferenzsysteme lassen sich vielfältig im Distanz- und Wechsel-/Hybridunterricht sowie im regulären Unterricht im Klassenzimmer einsetzen. Die Schulbehörde hat zu diesem Zweck einen Orientierungsrahmen für schulische Videokommunikation erarbeitet und den Schulen zur Verfügung gestellt.

Der erfolgreiche Einsatz von Videokonferenzen in der Schule erfordert einen rücksichtsvollen Umgang miteinander – wie bei anderen Themen in der Schule auch. Diese Hinweise sollen die Eltern, Schülerinnen und Schüler sowie weitere Angehörige der Schulgemeinschaft über den verantwortungsvollen Gebrauch dieser digitalen Konferenzen informieren.

Videokonferenzsoftware

Schulen nutzen grundsätzlich für Videokonferenzen und Videoübertragungen im Rahmen des Unterrichts die Software BigBlueButton. Diese Software steht z.B. in den Systemen „LMS Lernen Hamburg“ und „IServ“ zur Verfügung. Bei Ausfällen und bedeutsamen Funktionsstörungen kann eine Schule andere Softwarelösungen dafür nutzen. Dann trägt die Schule dafür Sorge, dass der Datenschutz gewährleistet ist und wird ggf. gesondert darüber informieren.

Respektvoller Umgang und Netiquette

Alles, was im Präsenzunterricht zum guten Ton gehört, gilt genauso im Online-Unterricht per Videokonferenz. Die Klassenregeln gelten weiter. Für Videokonferenzen ist es darüber hinaus sinnvoll, sich innerhalb der Klasse oder Schulgemeinschaft auf eine „Netiquette“ oder Regeln für digitale Kommunikation zu verständigen. Das heißt, dass alle Teilnehmenden ganz besonders auf den respektvollen Umgang miteinander achten und die Privatsphäre aller Beteiligten beachten. Bei der Übertragung von Zuhause sollten nur wirkliche nötige Informationen per Bild preisgegeben werden. Die Kamerafunktion muss immer dann aktiviert werden, wenn es pädagogische Gründe erfordern. Die Lehrkraft beachtet neben den Persönlichkeitsrechten auch die persönlichen Lebensumstände der Schülerinnen und Schüler.

Vertraulichkeit und Verbot von Aufzeichnungen

Der Videounterricht ist streng vertraulich und nicht öffentlich. Ohne ausdrückliche Erlaubnis darf niemand Inhalte aus dem Unterricht weitergeben. An Videokonferenzen dürfen nur Personen teilnehmen, die über individuelle Zugangsdaten Zutritt zum virtuellen Raum erhalten. Externe Personen dürfen nur eingeladen werden, wenn die Lehrkraft dies ausdrücklich erlaubt.

16 Quelle: Behörde für Schule und Berufsbildung Hamburg – B-Brief vom 1. April 2021

17 Siehe „Vierundzwanzigstes Gesetz zur Änderung des Hamburgischen Schulgesetzes vom 21. Januar 2021“ (vgl. HmbGVBl vom 29.01.2021, S. 45 ff., abrufbar: https://www.luewu.de/docs/gvbl/docs/2413.pdf).

Es ist verboten, Ton- und Videoaufnahmen zu machen.

Unerlaubte Ton- und Videoaufnahmen stellen eine schwere Verletzung der Persönlichkeitsrechte dar. Nach § 49 des Hamburgischen Schulgesetzes ist ein solches Fehlverhalten eine Störung des Schulfriedens und kann weitreichende rechtliche Konsequenzen zur Folge haben. Darauf weisen die Lehrkräfte alle ihre Schülerinnen und Schüler hin. Die Persönlichkeitsrechte der Schülerinnen und Schüler sowie der Lehrkräfte und das Recht am eigenen Bild stehen hier im Vordergrund.