

Datenschutzrechtliche Informationen

nach Art. 13 DSGVO

Im Folgenden sind die datenschutzrechtlichen Informationen zu den verschiedenen Nutzungsbereichen und Angeboten des August-Griese-Berufskolleg Löhne aufgeführt.

Der Verantwortliche im Sinne der DSGVO und anderer nationaler Datenschutzgesetze der Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen ist für die Schule:

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.de

Inhalt:

• Datenschutzrechtliche Informationen - Allgemein.....	2
• Datenschutzrechtliche Informationen - WLAN im AGB.....	4
• Nutzungsvereinbarung - Schooladmin Educloud.....	7
• Datenschutzrechtliche Informationen - EduCloud.....	11
• Datenschutzrechtliche Informationen - BigBlueButton.....	14
• Datenschutzrechtliche Informationen - Anfertigung von Fotos.....	16
• Datenschutzrechtliche Informationen - Webuntis / Untis-Mobile.....	18
• Datenschutzrechtliche Informationen - LMS Moodle.....	22
• Datenschutzrechtliche Informationen - Office 365.....	25

Datenschutzrechtliche Informationen - Allgemein

nach Art. 13 DSGVO

Verantwortlicher:

Der Verantwortliche im Sinne der DSGVO und anderer nationaler Datenschutzgesetze der Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen ist:

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.de

Datenschutzbeauftragte/r:

Der Datenschutzbeauftragte/r des Verantwortlichen ist:
Datenschutzbeauftragte/r für die Schulen des Kreises Herford
Christian Meyer
Schulamt des Kreises Herford
Amtshausstraße 3
32051 Herford
Tel.: 05732/3779
DSB-Schulen-HF@kreis-herford.de

Zweck lt. Art. 5 Abs. 1 lit. b DSGVO

Die erhobenen Daten dürfen nur für den Zweck der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülern¹ und Erziehungsberechtigten VO-DV I verarbeitet werden. Sie dienen zur Erfüllung gesetzlicher Anforderungen.

Schulen und Schulaufsichtsbehörden sind gemäß § 120 Abs. 1 Satz 1, Abs. 3 SchulG in Verbindung mit § 3 SchulG, im Übrigen nach den allgemeinen datenschutzrechtlichen Vorschriften, berechtigt und verpflichtet, personenbezogene Daten

1. der Schülerinnen und Schüler,
2. der Erziehungsberechtigten gemäß § 123 SchulG
3. der Verpflichteten gemäß § 41 SchulG
4. in § 36 SchulG genannte Schülerinnen und Schüler

in Dateien und/oder Akten zu verarbeiten, soweit die VO-DV I oder andere Rechtsvorschriften dies zulassen. Die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten sind in der Anlage zur VO-DV I genannt. Ferner finden sich in der VO-DV I weitere Vorgaben für die Datenverarbeitung.

https://www.schulministerium.nrw.de/docs/Recht/Schulrecht/Verordnungen/VO-DV_I.pdf

¹ Sofern in diesem Dokument die männliche Form (Schüler, Lehrer) gewählt wird, bezieht sie sich immer zugleich auf weibliche, männliche und diverse Personen. Auf eine Mehrfachbezeichnung wird zugunsten einer besseren Lesbarkeit verzichtet.

Empfänger nach Art. 13 Abs. 1 lit. e DSGVO

Die Daten werden nur von Empfängern verarbeitet, die auf Grund einer Rechtsgrundlage dazu berechtigt sind oder für die eine wirksame Einwilligung der Betroffenen vorliegt.

Übermittlung an Drittländer nach Art. 13 Abs. 1 lit. f DSGVO

Die Datenweitergabe in nicht EU-Mitgliedsstaaten ist unzulässig.

Dritterhebung nach Art. 14 Abs. 2 lit. f DSGVO

Sofern keine Dritterhebung erfolgt, erhalte ich die Daten aus dem EDV-System „Schulbewerbung.de“.

Speicherdauer lt. VO-DV I

Die Speicherdauer und die Löschfristen dienen der Erfüllung gesetzlicher Aufgaben und sind in der VO-DV I geregelt.

Betroffenenrechte lt. Art. 15 – 21 DSGVO

Sie haben ein Auskunfts-, Löschungs-, Berichtigungs-, Einschränkung- und Widerspruchsrecht sowie das Recht auf Datenübertragbarkeit. Das Löschungs-, Einschränkung- und Widerspruchsrecht ist insofern geschränkt, soweit ich die Daten zur Erfüllung gesetzlicher Anforderungen verarbeite.

Im Falle einer Einwilligung besteht das Recht, die Einwilligung jederzeit zu widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung wird hiervon nicht berührt (Art. 13 Abs. 2 lit. c DSGVO).

Bitte wenden Sie sich dazu an:

August-Griese-Berufskolleg Löhne

Die Schulleitung – vertr. durch Henning Tausch

Jahnstraße 54-68

32584 Löhne

Tel.: 05732/10840

E-Mail: agb@agb-loehne.de

Website: www.agb-loehne.de

Beschwerderecht:

Sie können sich jederzeit für Beschwerden an die Schulleitung, den Datenschutzbeauftragten oder an die Aufsichtsbehörde wenden.

Landesbeauftragte für Datenschutz und Informationsfreiheit

Nordrhein-Westfalen

Postfach 20 04 44

40102 Düsseldorf

Tel.: 0211/38424-0

Fax: 0211/38424-10

E-Mail: poststelle@ldi.nrw.de

Datenschutzrechtliche Informationen - WLAN im AGB

nach Art. 13 DSGVO

Am August-Griese-Berufskolleg nutzen Schüler und Lehrkräfte das schulische WLAN Netzwerk mit privaten Endgeräten und schulischen Leihgeräte und individualisierten Zugängen, um darüber auf Ressourcen im lokalen Netzwerk und im Internet zuzugreifen.

Damit das möglich ist, werden auch personenbezogene Daten der Benutzer verarbeitet. Hiermit möchten wir alle wichtigen Informationen dazu geben.

Für wen gelten diese Datenschutzhinweise?

Ausführliche Informationen

Informationen in vereinfachter Darstellung.

Diese Informationen zur Datenverarbeitung im Zusammenhang mit der Nutzung des schulischen WLAN mit privaten Endgeräten und/ oder schulischen Leihgeräten, gelten für alle schulischen Nutzer Schüler und Lehrkräfte.

Diese Informationen sind für alle WLAN Benutzer der Schule.

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

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.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 des schulischen WLAN mit privaten Endgeräten und/ oder schulischen Leihgeräten, geht es um folgende personenbezogene Daten:

- A.** Individualisierte Zugangsdaten (Benutzer, Passwort) werden für jeden Nutzer von der Schule erstellt.
- B.** Die Zuordnung zu Gruppen (Schüler, Lehrkräfte) erfolgt anhand von Informationen aus der Schulverwaltung.
- C.** Weitere Daten entstehen bei der Nutzung des WLAN mit einem privaten Endgerät und/ oder schulischen Leihgerät. Zu diesen Logdaten gehören:
 - a.** Zugriffsdaten (z.B. Datum, Uhrzeit und Dauer von Verbindungen mit dem WLAN, zur Verbindung genutzter Access Point),
 - b.** Aufgerufene IP Adressen/URLs von externen Ressourcen (Internet, LMS, schulische Online Plattformen, privat genutzte Apps) und IP Adressen/ Namen von internen Ressourcen (z.B. Netzlaufwerke, Drucker, ...),
 - c.** Gerätedaten (z.B. MAC Adresse des Endgerätes, Geräte name und -typ, -OS).

Du bekommst einen Benutzernamen und ein Passwort. Das sind Zugangsdaten. Bei der Nutzung des WLAN entstehen weitere Daten.

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

• Bereitstellung eines individualisierten Zugangs zum schulischen WLAN zur Nutzung im Unterricht und zur Vor- und Nachbereitung von Unterricht. • Verwaltung von Rollen und Rechten der Benutzer im schulischen Netzwerk entsprechend der Zugehörigkeit zu Gruppen (Schüler / Lehrkraft), • Technische Bereitstellung des schulischen WLAN, • Sicherheit und Funktionalität des schulischen WLAN (z.B. Filterung).	Der WLAN Router muss wissen, wer das WLAN benutzen darf.
Die Verarbeitung der oben genannten personenbezogenen Daten erfolgt auf der Rechtsgrundlage von: • Art. 6 Abs. 1 lit e), Abs. 3 lit b) DSGVO in Verbindung mit SchulG NRW, VO-DV I, VO-DV II	Die Schule speichert deine Kontodaten solange du hier Schüler bist.

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

Die Nutzung des schulischen WLAN erfordert eine technische Betreuung durch [Mitarbeiter des Schulträgers/ Mitarbeiter eines IT Dienstleisters].	Deine Daten bleiben immer bei der Schule. Mitarbeiter des Schulträgers/ IT Dienstleisters dürfen mit deinen Daten nur machen, was deine Schule erlaubt.
Auftragsverarbeiter - nach Weisung durch die Schulleitung • Von der Schule / vom Schulträger beauftragten Dienstleister bzw. beauftragten Mitarbeiter.	
Innerhalb der Schule wird der Zugriff auf die Daten im Zusammenhang mit der Nutzung des WLAN durch ein Rechte- und Rollenkonzept geregelt. • Schulleitungsmitglieder - alle Daten, ohne administrative Rechte, jedoch nur im Verdachtsfall einer Straftat im vier-Augen-Prinzip und nach vorheriger Information des Betroffenen • Schulische Administratoren - alle Daten aller Personen (auf Weisung der Schulleitung)	Die Schulleitung darf alles sehen, wenn jemand etwas Schlimmes getan hat. Das ist normal. Unser Administrator darf alles sehen. Das darf er nur, weil die Schulleitung es ihm erlaubt.
Personen von außerhalb der Schule erhalten nur Zugriff auf Daten, wenn ein Gesetz es ihnen gestattet. • Erziehungsberechtigte und (ehemalige) Schüler (Auskunftsrecht Art. 15 DSGVO) • Ermittlungsbehörden im Fall einer Straftat.	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.

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

Nein. Alle persönlichen Daten, die im Zusammenhang mit der Nutzung des schulischen WLAN anfallen, bleiben in Deutschland.	Nein.
---	-------

Findet eine automatisierte Entscheidungsfindung statt?

Nein.	Nein.
-------	-------

Wie lange werden meine Daten gespeichert?

Die Benutzerdaten von Schülern und Lehrkräften im Zusammenhang mit dem individualisierten Zugang zum schulischen WLAN über ein privates Endgerät und/ oder schulisches Leihgerät (Kontodaten) werden solange gespeichert wie diese	Solange du dein WLAN Konto nutzt, speichert die Schule deine Kontodaten. Wenn du die Schule verlässt, löschen wir deine
--	---

- das schulische WLAN 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 zum schulischen WLAN, Verlassen Schule bzw. Ende des Dienstes an Schule werden die Kontodaten des Benutzers innerhalb von sechs Wochen endgültig aus der Verwaltung des WLAN gelöscht. - Daten im Zusammenhang mit der Erstellung von Verwaltung von Benutzerkonten für die Nutzung des schulischen WLAN, die in der Schulverwaltung vorliegen, werden entsprechend VO-DV I §9 bzw. VO-DV II §9 für 5 Jahre aufbewahrt.	Kontodaten. Wir löschen deine Zugangsdaten innerhalb von 6 Wochen.
Logdaten, die im Zusammenhang mit der Nutzung des schulischen WLAN entstehen, werden nach 7 Tagen automatisiert gelöscht.	Nutzungsdaten werden immer nach 7 Tagen gelöscht.
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.	Frage deine Schule, wenn du wissen willst, welche Daten es von dir gibt, du einen Fehler gefunden hast, du möchtest, dass etwas gelöscht wird.
Recht zur Beschwerde bei der Aufsichtsbehörde	
Zudem steht Ihnen ein Beschwerderecht bei der Datenschutzaufsichtsbehörde, der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen zu.	Du hast ein Problem mit deinen Daten. In der Schule kann man dir nicht helfen. Dann kannst du dich bei den Datenschützern des Landes Nordrhein-Westfalen beschweren.

Nutzungsvereinbarung - Schooladmin Educloud

Die „Schooladmin Educloud“ nutzt als Basis das Open Source Projekt Nextcloud, welches absolut datenschutzkonform ist. Nextcloud wurde für den lokalen Betrieb entwickelt, also z.B. auf dem Schulserver. Die schooladmin Educloud stellt der Schule alle notwendigen Services und Daten so zur Verfügung, dass sie mit jedem Endgerät jederzeit genutzt werden können.

Was ist eine Nutzungsvereinbarung und worum geht es hier?

Ausführliche Informationen

Informationen in vereinfachter Darstellung.

Die Nutzungsvereinbarung legt die Regeln fest, an welche sich alle Personen halten müssen, welche die EduCloud der Schule nutzen.

Vereinbarung heißt: Wir einigen uns auf Regeln.

Die Vereinbarung erklärt dir unsere Educloud Regeln.

Für wen gilt diese Nutzungsvereinbarung?

Die Nutzungsvereinbarung gilt für Schüler, nachfolgend "Benutzer" genannt, welche die von der Schule bereitgestellte Educloud zur elektronischen Datenverarbeitung nutzen.

Die Vereinbarung ist für Schüler.

Wie lange gilt die Nutzungsvereinbarung?

Dem Benutzer wird innerhalb seiner Schulzeit ein Benutzerkonto in der schulischen Educloud zur Verfügung gestellt. Beim Verlassen der Schule wird dieses Benutzerkonto deaktiviert und gelöscht.

Die Vereinbarung gilt für deine Schulzeit an unserer Schule.

Worauf bezieht sich die Nutzungsvereinbarung?

Zum Umfang des von der Schule für die Benutzer kostenlos bereitgestellten Paketes gehören:

- Zugang zur schulischen Educloud mit
 - einem persönlichen Benutzerkonto
 - verschiedenen Educloud Diensten wie z.B. Dateimanager. (Anzahl und Umfang der innerhalb Educloud durch die Schule angebotenen Dienste richten sich nach dem aktuellen Nutzungskonzept, der Weiterentwicklung der Educloud sowie der technischen Verfügbarkeit und können damit Änderungen unterworfen sein.)

Für die Educloud bekommst du einen Benutzer-Namen und ein Passwort.

Damit meldest du dich an. In der Educloud kannst du Dateien speichern.

Was sind personenbezogene Daten?

Passwörter

- müssen so sicher sein, dass sie nicht erratbar sind. Sie müssen aus mindestens 8 Zeichen bestehen und eine Zahl, einen Großbuchstaben und ein Sonderzeichen enthalten.
- Es darf kein Passwort verwendet werden, das bereits für andere Dienste genutzt wird.

Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum Schulnetz und damit auch zur schulischen Educloud 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

Verrate niemandem dein Passwort. Deine Eltern dürfen es aber wissen. Wenn doch jemand dein Passwort kennt, ändere es schnell. Ein Lehrer hilft dir bei Problemen.

verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist die Klassenleitung 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 die Klassenleitung zu informieren. • Nach Ende der Unterrichtsstunde oder Arbeitssitzung an einem schulischen Rechner meldet sich der Benutzer vom PC ab (ausloggen).	<i>Vielleicht findest du einmal den Benutzer-Namen und das Passwort von einem anderen Schüler. Du darfst das nicht benutzen. Sag dem anderen Schüler Bescheid.</i>
Personenbezogene Daten	
Für die Nutzung von personenbezogene Daten wie dem eigenen Namen, 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.	<i>Speichere in der Educloud nur Daten, die du wirklich brauchst. Geheimnisse gehören nicht in die Educloud.</i>
Persönliches Profil • Im persönlichen Profil können Benutzer zusätzliche Informationen eingeben. Private Informationen tragen Benutzer auf eigene Verantwortung ein. Über die Rechtevergabe können sie steuern, ob eingetragene Informationen nur für sie selbst sichtbar sind (privat) oder für alle Benutzer der schulischen Educloud und von der Schule als vertrauenswürdig eingestufte andere Educlouds, z.B. von Schulen, mit denen man kooperiert (Kontakte). Die Einstellung öffentlich, mit welcher die Informationen über Internet für jedermann auffindbar sind, ist nicht zulässig.	<i>Mein Profil</i> <i>In der Educloud kannst du etwas über dich schreiben. Das heißt Profil.</i>
Speicherorte • Innerhalb der Educloud hat jeder Benutzer seinen persönlichen Bereich. Das hier gespeichert ist, kann nur der Benutzer selbst sehen. Benutzer haben außerdem Zugriff auf Ordner und Verzeichnisse in Gruppen, welchen sie zugeordnet sind. Dazu gehören beispielsweise die Verzeichnisse von Klassen und Kursen.	<i>Wo kann ich meine Dateien speichern?</i> <i>Für deine Dateien hast du einen eigenen Bereich. Nur du kannst dort hinein schauen.</i> <i>Auch deine Klasse hat einen Ordner. Du kannst Dateien dort speichern. Dein Lehrer sagt dir, was du dort speichern darfst.</i>
Freigabe von Dateien Benutzer können Inhalte in den Verzeichnissen der Educloud entsprechend ihrer Berechtigungen mit Nutzern innerhalb und außerhalb der schulischen Instanz über Dateifreigaben teilen. Datenschutz- und urheberrechtliche Vorgaben sind dabei zu beachten.	<i>Teilen von Dateien</i> <i>Du kannst Dateien mit anderen teilen. Teilen geht in der Schule und im Internet. Viele Bilder, Texte, Musik und Videos gehören anderen Leuten. Du darfst sie nicht teilen. Bist du nicht sicher? Dann frage deine Lehrer.</i>
Urheberrecht	
• Bei der Nutzung der schulischen Educloud sind die geltenden Bestimmungen des Urheberrechtes zu beachten. Fremde Inhalte,	<i>Die meisten Dinge im Internet gehören anderen Menschen. Sie</i>

deren Nutzung nicht durch freie Lizenzen wie Creative Commons, GNU oder Public Domain zulässig ist, dürfen ohne schriftliche Genehmigung der Urheber nicht in der schulischen Educloud gespeichert werden, außer ihre Nutzung erfolgt im Rahmen des Zitatrechts.	<i>haben die Bilder, Filme und Musik gemacht. Du darfst diese Dinge nicht in Educloud speichern.</i>
• Fremde Inhalte (Texte, Fotos, Videos, Audio und andere Materialien), die nicht unter freien Lizenzen wie Creative Commons, GNU oder Public Domain stehen, dürfen nur mit der schriftlichen Genehmigung des Urhebers veröffentlicht werden. Dieses gilt auch für digitalisierte Inhalte (eingescannte oder abfotografierte Texte und Bilder) sowie Audioaufnahmen von urheberrechtlich geschützten Musiktiteln (GEMA). Bei vorliegender Genehmigung ist bei Veröffentlichungen auf einer eigenen Website der Urheber zu nennen, wenn dieser es wünscht. Bei der Veröffentlichung von Creative Commons und GNU lizenzierten Inhalten sind die Nutzungsvorgaben der Urheber in der von diesen angegebenen Form umzusetzen.	<i>Du darfst diese Dinge nicht mit anderen teilen. Im Unterricht zeigen wir dir sichere Bilder, Filme, Musik und Texte. Die darfst du benutzen und teilen.</i>
• Bei der unterrichtlichen Nutzung von freien Bildungsmaterialien (Open Educational Resources - OER) sind die jeweiligen Lizenzen zu beachten und entstehende neue Materialien oder Lernprodukte bei einer Veröffentlichung entsprechend der Bedingungen der vergebenen Creative Commons Lizenzen zu lizenzieren.	<i>OER erklären wir dir im Unterricht.</i>
• Bei von der Schule über die Educloud zur Verfügung gestellten digitalen bzw. digitalisierten 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 bzw. digitalisierter Inhalte von Lehrmittelverlagen zulässig.	<i>In unserer Educloud haben wir Sachen aus dem Schulbuch. Das muss in der Educloud bleiben.</i>
• Stoßen Benutzer in der schulischen Educloud auf urheberrechtlich geschützte Materialien, deren Nutzung nicht den beschriebenen Vorgaben entspricht, sind sie verpflichtet, dieses bei einer verantwortlichen Person anzuzeigen.	<i>Ein anderer hält sich nicht an die Regeln. Du siehst das in der Educloud. Du findest etwas. Sage es einem Lehrer.</i>
• Die Urheberrechte an Inhalten, welche Benutzer eigenständig erstellt haben, bleiben durch eine Ablage oder Bereitstellung in der schulischen Educloud unberührt.	<i>Deine Texte, deine Bilder, deine Musik und deine anderen Sachen gehören dir. Das ist auch in unserer Educloud so.</i>
Unzulässige Inhalte und Handlungen - Was ist nicht erlaubt?	
• Benutzer sind verpflichtet, bei der Nutzung der schulischen Educloud geltendes Recht einzuhalten.	<i>In der Educloud gelten die Gesetze unseres Landes.</i>
• Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die schulische Educloud zu erstellen, abzurufen, zu speichern oder zu verbreiten.	<i>Nackte Haut, Gewalt, Nazi-Sachen und andere schlimme Sachen sind in der Educloud verboten.</i>
• Die geltenden Jugendschutzvorschriften sind zu beachten. Siehe dazu auch Jugendmedienschutz, Wikipedia .	<i>Es gibt Filme, Bilder, Musik und Texte für Kinder und Jugendliche. Die sind OK in unserer Educloud.</i>
• Die Verbreitung und das Versenden von belästigenden, beleidigenden, verleumderischen nötigenden, herabwürdigenden,	<i>Sei nett und höflich zu allen in der Educloud.</i>

verletzenden oder bedrohenden Inhalten ist unzulässig.	
Was passiert, wenn ich mich nicht an die Regeln halte?	
Im Falle von Verstößen gegen diese Nutzungsordnung behält sich die Schulleitung des AGB das Recht vor, den Zugang zu einzelnen oder allen Bereichen innerhalb der schulischen Educloud zu sperren und die Nutzung schulischer Endgeräte zu untersagen. Davon unberührt behält sich die Schulleitung weitere disziplinarische Maßnahmen gegenüber Schülern vor.	<i>Wer die Regeln nicht einhält, darf nicht mehr die Educloud. Wir informieren dann die Erziehungsberechtigte. Vielleicht gibt es auch eine Strafe.</i>

Datenschutzrechtliche Informationen - EduCloud

nach Art. 13 DSGVO

Am AGB nutzen Schüler und Lehrkräfte die Educloud als Arbeitsplattform. Damit das möglich ist, werden auch personenbezogene Daten der Benutzer verarbeitet. Hiermit möchten wir Ihnen / dir alle wichtigen Informationen dazu geben.

Für wen gelten diese Datenschutzhinweise?

<i>Ausführliche Informationen</i>	<i>Informationen in vereinfachter Darstellung.</i>
Diese Informationen zur Datenverarbeitung im Zusammenhang mit der Nutzung von Educloud gelten für alle schulischen Nutzer von Educloud, Schüler und Lehrkräfte.	<i>Diese Informationen sind für alle Educloud Benutzer der Schule.</i>

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

August-Griese-Berufskolleg Löhne Die Schulleitung – vertr. durch Henning Tausch Jahnstraße 54-68 32584 Löhne Tel.: 05732/10840 E-Mail: agb@agb-loehne.de Website: www.agb-loehne.de	<i>Bei Fragen zum Schutz deiner Daten hast oder Problemen, rede mit diesen Personen.</i>
---	--

Woher kommen meine Daten und welche Daten werden verarbeitet?

• Anmeldedaten werden für jeden Nutzer von der Schule erstellt. • Die Zuordnung zu Gruppen und die damit verbundenen Rollen und Rechte erfolgt anhand von Informationen aus der Schulverwaltung. Ein Teil der Daten dort wurde bei der Anmeldung an der Schule angegeben. • Weitere Daten entstehen bei der Nutzung der Educloud im Unterricht und bei der Vor- und Nachbereitung des Unterrichts.	<i>Die Daten kommen von dir selbst. Sie kommen vom Schulbüro.</i>
• Benutzerdaten (z.B. Anmeldenamen, Passwort, Gruppenzugehörigkeit) • Vom Benutzer erzeugte Inhalts- und Kommunikationsdaten (z.B. Dokumente, Audioaufnahmen und Nachrichten) • Technische Nutzungsdaten (z.B. erzeugte Dateien, Versionen, Fehlermeldungen)	<i>Wenn du Educloud benutzt, entstehen Daten. Du siehst sie nicht alle.</i>

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

• Durchführung, Vor- und Nachbereitung von Unterricht • Verwaltung von Rechten und Rollen der Benutzer entsprechend der Funktion (Schüler/ Lehrkraft/Lehrerrat/SV) und der Zugehörigkeit zu Klassen und Gruppen • Technische Bereitstellung von für die Verwaltung und Nutzung der Educloud erforderlichen Diensten • Sicherheit und Funktionalität dieser Dienste	<i>Die Educloud braucht deine Daten, damit du dort lernen und arbeiten kannst. Deine Daten helfen der Educloud. Sie weiß dann, in welche Klasse du gehörst.</i>
• Die Verarbeitung sämtlicher Daten erfolgt auf der Grundlage einer Einwilligung (Artikel 6 Abs. 1 lit. a DSGVO) durch die Betroffenen.	<i>Deine Daten sind in der Educloud, solange du damit einverstanden bist.</i>

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

Auftragsverarbeiter - nach Weisung durch die Schulleitung • Von der Schule/ vom Schulträger beauftragter Dienstleister.	<i>Deine Daten bleiben immer bei der Schule.</i>
Innerhalb der Schule wird der Zugriff auf die Daten im Zusammenhang mit der Nutzung der Educloud durch das Rechte- und Rollenkonzept geregelt. • Schulleitung - alle technischen und öffentlichen Daten; Daten im persönlichen Nutzerverzeichnis 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, • Schulischer Administrator - alle Daten aller Personen (auf Weisung der Schulleitung) • Lehrkräfte - Eigene Daten und Daten von Schülern und Lehrkräften entsprechend ihrer Funktion und Freigaben durch die Personen selbst • Schüler - Eigene Daten und Daten von Mitschülern entsprechend Freigaben von Lehrkräften oder Mitschülern	<i>Du bist der Chef von deinen Daten. Lehrer und andere Schüler dürfen deine Daten sehen, wenn du es ihnen erlaubst. Unser Administrator kann alles sehen. Das darf er nur, wenn die Schulleitung es erlaubt.</i>
Personen von außerhalb der Schule erhalten nur Zugriff auf Daten, wenn ein Gesetz es ihnen gestattet • Erziehungsberechtigte bei Freigabe durch Schüler • Erziehungsberechtigte und (ehemalige) Schülern (Auskunftsrecht Art. 15 DSGVO) • Ermittlungsbehörden im Fall einer Straftat	<i>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.</i>

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

Nein. Die Server unseres Anbieters stehen in Deutschland.	<i>Nein.</i>
---	--------------

Findet eine automatisierte Entscheidungsfindung statt?

Nein, in den Diensten der Educloud 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.	<i>Nein! In unserer Educloud entscheiden nur Menschen, keine Computer.</i>
---	--

Wie lange werden meine Daten gespeichert?

Die Benutzerdaten von Schülern und Lehrkräften werden solange gespeichert wie diese • die Educloud 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 der Educloud, Verlassen Schule bzw. Ende des Dienstes an Schule oder Widerspruch in die Verarbeitung werden die Daten des Benutzers innerhalb von sechs Wochen endgültig aus der Educloud gelöscht. [Name des Anbieters] löscht sämtliche Daten danach von allen Servern und Sicherheitskopien in einem Zeitraum von 6 Monaten. • Unterrichtsdaten werden am Schuljahresende gelöscht. Inhalte der Benutzer bleiben davon unberührt. Daten im	<i>Solange du die Educloud der Schule nutzt, speichert sie deine Daten. Wenn du die Schule verlässt oder deine Einwilligung widerrufst, löschen wir deine Daten. Erst löschen wir die Daten. Dann löscht Educloud die Daten auch noch einmal. Das dauert etwa 6 Monate. Danach ist alles weg. Was du in der Educloud selbst gemacht hast, kannst du immer auch selbst löschen.</i>
--	--

Zusammenhang mit einem e-Portfolio werden für die gesamte Schulzeit gespeichert. • Daten im Zusammenhang mit der Erstellung von Verwaltung von Benutzerkonten für die Nutzung der Educcloud, 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 erstellte Inhalte eigenständig zu 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.	<i>Du hast eine Frage zu deinen Daten. Dann sprich deine Schule an. Frage nach, 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.</i>
Recht zur Beschwerde bei der Aufsichtsbehörde	
Zudem steht Ihnen ein Beschwerderecht bei der Datenschutzaufsichtsbehörde, der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen zu.	<i>Du hast ein Problem mit deinen Daten. In der Schule kommst wirklich nicht mehr weiter. Dann kannst du dich bei den Datenschützern des Landes Nordrhein-Westfalen beschweren.</i>

Datenschutzrechtliche Informationen - BigBlueButton

nach Art. 13 DSGVO

Hier informieren wir Sie über die zur Nutzung von des Videokonferenzsystems BigBlueButton erforderliche Verarbeitung von personenbezogenen Daten.

Wer ist verantwortlich für die Verarbeitung der Daten und wer kann Fragen zum Datenschutz beantworten?

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.de

Datenschutzbeauftragte/r:

Der Datenschutzbeauftragte/r des Verantwortlichen ist:
Datenschutzbeauftragte/r für die Schulen des Kreises Herford
Christian Meyer
Schulamt des Kreises Herford
Amtshausstraße 3
32051 Herford
Tel.: 05732/3779
DSB-Schulen-HF@kreis-herford.de

Zu welchem Zweck sollen die Daten verarbeitet werden?

Die Verarbeitung ist erforderlich zur Nutzung von BigBlueButton, einer Videokonferenz-Plattform, zur Durchführung von Online-Unterrichtseinheiten in der Lerngruppe und individueller Betreuung und Beratung in Kleingruppen oder Einzeltreffen zwischen Schüler und Lehrkraft.

Welche personenbezogenen Daten werden bei Teilnahme an einer BigBlueButton Videokonferenz verarbeitet?

Bei der Teilnahme an einer BigBlueButton Videokonferenz ohne eigenes Nutzerkonto werden neben Bild- und Tondaten, zusätzliche Daten zur Konferenz verarbeitet: Name des Raumes des Teilnehmers und Informationen zum genutzten Endgerät. Je nach Nutzung der Funktionen in einer Videokonferenz fallen Inhalte von Chats, gesetzter Status, Eingaben bei Umfragen, Beiträge zum geteilten Whiteboard, durch Upload geteilte Dateien und Inhalte von Bildschirmfreigaben an. Eine Speicherung von Videokonferenzen und Inhalten durch die Schule erfolgt nicht.

Wer hat Zugriff auf die personenbezogenen Daten?

Alle Teilnehmer einer Videokonferenz haben Zugriff im Sinne von Sehen, Hören und Lesen auf Inhalte der Videokonferenz, Chats, geteilte Dateien, Bildschirmfreigaben und Beiträge auf Whiteboards. Der Anbieter hat Zugriff auf die verarbeiteten Daten im Rahmen der Auftragsverarbeitung und auf Weisung der Schulleitung.

An wen werden die Daten übermittelt?

Die BigBlueButton-Instanz wird direkt vom August-Griese-Berufskolleg Löhne betrieben. Im Sinne des Datenschutzrechts findet somit keine Übermittlung statt.

Wie lange werden die Daten gespeichert?

Die Schule speichert keine personenbezogenen Daten im Zusammenhang mit der Nutzung von BigBlueButton. Videokonferenzen und Chats werden nicht aufgezeichnet und weder durch Schule noch den Anbieter gespeichert. Die Inhalte von Chats, geteilte Dateien und Whiteboards werden in der Plattform gelöscht, sobald ein Konferenzraum geschlossen wird.

Datenschutzrechtliche Informationen - Anfertigung von Fotos zur Verwendung innerhalb des elektronischen Klassenbuchs (Webuntis) und zur Erstellung eines Schülerschweises nach Art. 13 DSGVO

Wer ist verantwortlich für die Verarbeitung der Daten und wer kann Fragen zum Datenschutz beantworten?

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.de

Datenschutzbeauftragte/r:

Der Datenschutzbeauftragte/r des Verantwortlichen ist:
Datenschutzbeauftragte/r für die Schulen des Kreises Herford
Christian Meyer
Schulamt des Kreises Herford
Amtshausstraße 3
32051 Herford
Tel.: 05732/3779
DSB-Schulen-HF@kreis-herford.de

Verarbeitung von personenbezogenen Daten und Anfertigung von Fotos

Die Schule fertigt zur Erstellung von Schülerschweisen sowie zur Nutzung innerhalb der elektronischen Klassenbuchs (Webuntis) Portraitfotos an. Verarbeitet werden außer dem Foto noch Name, Vorname und eine interne Schüler ID.

Die Rechteeräumung an den Fotos erfolgt ohne Vergütung und umfasst auch das Recht zur Bearbeitung, soweit die Bearbeitung nicht entstehend ist.

Diese Einwilligung kann für die Zukunft jederzeit widerrufen werden. Dabei kann der Widerruf auch nur auf einen Teil der Datenarten oder Fotos 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 werden entsprechende Daten nicht für den oben genannten Zweck verwendet. Soweit die Einwilligung nicht widerrufen wird, gilt sie bis der Schülerschweis erstellt ist.

Anlassbezogene Veröffentlichung von Texten, Fotos und Videos

In geeigneten Fällen wollen wir Informationen über Ereignisse aus unserem Schulleben – auch personenbezogen – der Öffentlichkeit zugänglich machen. Wir beabsichtigen daher, insbesondere im Rahmen der pädagogischen Arbeit oder von Schulveranstaltungen entstehende Texte, Fotos oder Videos zu veröffentlichen. Neben Klassenfotos kommen hier etwa personenbezogene Informationen über Schulausflüge, Schülerfahrten, Schüleraustausche, (Sport-)Wettbewerbe, Unterrichtsprojekte oder den „Tag der Offenen Tür“ in Betracht.

Bei einer Online-Veröffentlichung, beispielsweise auf der Schulwebseite oder in der digitalen Lokalpresse, sind personenbezogene Daten, einschließlich Fotos und Videos, weltweit und dauerhaft zugänglich. Sie könnten über Suchmaschinen gefunden werden. Es besteht die Möglichkeit, dass Dritte diese Daten mit anderen im Internet verfügbaren Informationen kombinieren, ein Persönlichkeitsprofil erstellen, die Daten modifizieren oder sie für andere Absichten nutzen.

Die gegebene Einwilligung kann jederzeit für die Zukunft komplett widerrufen werden oder auch nur für einen Teil der Medien, Datenarten oder Fotos. Ein Widerruf beeinflusst nicht die Rechtmäßigkeit bereits erfolgter Verarbeitungen auf Basis der Einwilligung. Bei Druckmaterialien ist ein Widerruf nach Freigabe zum Druck nicht mehr möglich. Bei einem Widerruf werden betroffene Daten online nicht mehr verwendet und umgehend gelöscht. Sofern nicht widersprochen wird, bleibt die Zustimmung für die Dauer der Schulzugehörigkeit bestehen.

Datenschutzrechtliche Informationen - Webuntis / Untis-Mobile

nach Art. 13 DSGVO

Die folgende Datenschutzerklärung informiert Sie über die Verarbeitung und den Schutz von (personenbezogenen) Daten in den Programmen Webuntis und Untis-Mobile. Die Informationen stammen von der Untis GmbH, dem Herausgeber und Produzenten dieser Programme.

1. Allgemeines

Ihre Daten, die bei WebUntis bzw. Untis-Mobile verarbeitet werden, sind bei uns (das ist die Untis GmbH) in sicheren Händen! Wir sind dazu verpflichtet, Ihre im Zuge unserer Geschäftsbeziehung verarbeiteten personenbezogenen Daten zu schützen und nehmen diesen Auftrag auch ernst. Bitte nehmen Sie sich Zeit für diese Datenschutzinformation und bekommen Sie ein Bild darüber, warum wir Ihre Daten erheben und in welcher Form wir sie verarbeiten.

- Wir verarbeiten personenbezogene Daten zum Betrieb jener Systeme, auf denen unsere Produkte bereitgestellt werden. Hierbei sind wir (je nach konkreter Funktionalität und der unserem Vertragspartner geschuldeten Leistung) Verantwortlicher oder Auftragsverarbeiter iSd DSGVO.
Siehe dazu Punkt 3
- Wir verarbeiten personenbezogene Daten bei WebUntis und Untis-Mobile im Auftrag und auf Weisung unserer Vertragspartner (Auftragsverarbeiter iSd DSGVO).

2. Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die sich auf natürliche Personen (Schüler*innen, Erziehungsberechtigte von Schüler*innen oder Lehrer*innen) beziehen, deren Identität identifiziert oder identifizierbar ist (z.B.: Name, Kontaktdaten, Rechnungsdaten, IP-Adresse).

3. Betrieb der Systeme, auf denen wir unsere Produkte zur Verfügung stellen

Um unsere Produkte anbieten zu können, werden hierfür folgende Informationen verarbeitet, die grundsätzlich einen Bezug zum jeweiligen Benutzer ermöglichen:

- Benutzername
- Benutzer-ID
- Datum und Uhrzeit des Aufrufs
- Aufgerufene URL
- Referrer URL
- Bildungseinrichtung
- IP-Adresse
- Verwendeter Browser
- Verwendetes Betriebssystem
- requestId
- traceId

Zur Übermittlung der Daten wird TLS Verschlüsselung verwendet.

Diese Daten werden für die zuverlässige und sichere zur Verfügungstellung unserer Produkte verarbeitet und nach Ablauf von sechs Monaten ab Erhebung gelöscht. Die Aufbewahrung für sechs Monate erfolgt um etwaige auftretende technische Probleme identifizieren, zuordnen und beheben zu können. Darüber hinaus können sie zur Unterstützung der Ermittlungsbehörden bei der Aufklärung von Straftaten dienen.

4. Datenverarbeitung im Rahmen von WebUntis und Untis-Mobile

Sowohl WebUntis als auch Untis-Mobile sind Plattformen für die selbe Datenbank und beinhalten somit dieselben Datensätze. Die zur Verfügung stehenden Funktionalitäten sind weitestgehend gleich.

Bei der Benutzung von WebUntis oder Untis-Mobile erfolgt die Verarbeitung Ihrer personenbezogenen Daten aufgrund der mit dem jeweiligen Verantwortlichen (dies ist jene Bildungseinrichtung, die Sie besuchen, Ihr Kind besucht bzw. an der Sie lehren) abgeschlossenen Auftragsverarbeitervereinbarung gemäß Art 28 DSGVO.

Unabhängig von der jeweiligen Benutzerrolle und den damit verbundenen Berechtigungen wird seitens der Schule festgelegt, welche Daten als erforderlich erachtet werden und wem diese zugänglich gemacht werden. Wir stellen die Plattformen zur Verfügung, damit die Anforderungen der jeweiligen Einrichtung realisiert werden können. Die Plattformen umfassen – je nach jeweiliger Benutzerberechtigung – folgende Funktionalitäten:

- Raumbuchungen
- Stunden- und Vertretungsplanung
- Elektronisches Klassenbuch
- Sprechtag-Planung
- Kursanmeldung

Eine vollständige Darstellung der aktuell verfügbaren Funktionen finden Sie [hier](#).

Einsatz von Matomo

Wir verwenden [Matomo](#) für die Messung der Nutzung und Leistung unserer Produkte WebUntis und Untis-Mobile, um datengestützte Entscheidungen zur Identifikation von Verbesserungspotenzialen zu ermöglichen:

- Es werden hierfür keine personenbezogenen Daten verarbeitet,
- IP Adressen werden anonymisiert,
- Daten am Endgerät: Da Matomo nur Stichproben-artig aktiviert wird, speichert es im local storage im Schlüssel ANALYTICS-config, ob es aktiviert oder deaktiviert ist,
- es wird eine ID generiert, über welche sich die User Journey ("eine Szenario-basierte Abfolge von Schritten, die ein Benutzer unternimmt, um ein übergeordnetes Ziel mit einem Produkt zu erreichen") eines Benutzers ausschließlich zwischen dem Web-Client (WebUntis) und Mobile Clients (Untis-Mobile Android- oder iOS-App) verfolgen lässt.

Untis-Mobile

Bei der Verwendung von Untis-Mobile werden keine zusätzlichen Informationen an uns übermittelt. All jene von Untis-Mobile erzeugten Daten, die über jene von WebUntis hinausgehen, werden ausschließlich auf dem Gerät des Benutzers gespeichert; eine Synchronisierung dieser Daten mit den Untis-Systemen findet NICHT statt.

Im Rahmen einer vertraglichen Beziehung mit Ihnen werden wir Ihre Daten aufgrund unternehmens- und steuerrechtlicher Dokumentationspflichten gemäß § 212 UGB bzw. § 132 BAO grundsätzlich für die Dauer von sieben Jahren (ab Ende des jeweiligen Geschäftsjahres) aufbewahren. In begründeten Einzelfällen, etwa zur Geltendmachung und Abwehr von konkreten Rechtsansprüchen, können wir Ihre Daten auch bis zu 30 Jahre nach Beendigung der Geschäftsbeziehung speichern. Personenbezogene Daten werden keinen Empfängern offengelegt.

Hinsichtlich all jener Verarbeitungsvorgänge, für welche wir nicht Verantwortlicher iSd DSGVO sind, sondern Auftragsverarbeiter, verweisen wir auf die Datenschutzinformationen der jeweiligen verantwortlichen Bildungseinrichtung.

Untis-Mobile nutzt von Firebase (ein Produkt von Google) bereitgestellte Dienste:

- Firebase Cloud Messaging, für das Versenden von Push-Nachrichten,

- Firebase Crashlytics, für die Auswertung automatisch erstellter Fehlermeldungen (z.B. bei Abstürzen),
- Firebase Remote Config, für Konfigurationsanpassungen in der App, ohne eine neue Version im Store veröffentlichen zu müssen.

In Untis-Mobile können Berechtigungen abgefragt werden. Diese Berechtigungen können im Nachhinein in den Applikationseinstellungen konfiguriert werden. Sofern Sie die Berechtigungen nicht erteilen, ist die Verwendung von Untis-Mobile nur eingeschränkt möglich.

- Kamera: Der Zugriff auf die Kamera wird benötigt um Fotos, Videos und QR-Codes zu verarbeiten. Fotos und Videos werden für die Datenübertragung an WebUntis benötigt. QR-Codes werden für die Anmeldung genutzt.
- Fotos und Videos: Der Zugriff auf Fotos und Videos werden zur Datenübertragung an WebUntis benötigt.
- Push Notifications: Mit Push-Notifications wird der Benutzer über relevante Informationen benachrichtigt. Beispielsweise über Änderungen im Stundenplan.

Sofern Sie die Berechtigungen nicht erteilen bzw. nach der Installation deaktivieren, ist die Verwendung von Untis-Mobile nur eingeschränkt möglich.

Wir weisen weiters darauf hin, dass Untis-Mobile keine Werbung beinhaltet (der diesbezügliche Hinweis durch den Google PlayStore erfolgt aufgrund der Verknüpfung von Untis-Mobile).

5. Automationsunterstützte Entscheidungsfindung

Wir führen mit Ihren Daten keine Verarbeitungen durch, bei denen es zu Entscheidungen kommt, die auf ausschließlich automatisierten Verarbeitungen (einschließlich Profiling) beruhen und die Ihnen gegenüber rechtliche Wirkung entfalten oder Sie in ähnlicher Weise erheblich benachteiligen (Art 22 DSGVO). Jede etwaige Entscheidung mit entsprechender Wirkung wird von einer natürlichen Person getroffen.

6. Erhebung von Daten aus anderen Quellen (Information gemäß Art 14 DSGVO)

Es werden keine Daten von anderen Quellen erhoben. Wir verwenden ausschließlich jene Informationen, die Sie bei der Benutzung eingeben bzw. bereitstellen (z.B.: gespeicherte Hausaufgaben oder Abwesenheitsmeldungen).

Abhängig von der jeweiligen Funktion findet eine Weiterverarbeitung von erhobenen und verarbeiteten, Daten statt (z.B.: Anmeldung zur Sprechstunde anhand der Zuordnung der Informationen zu Schüler*innen und Lehrer*innen).

Bei der Verwendung werden keine zusätzlichen Informationen an uns übermittelt. Alle erzeugten Daten, die über jene von WebUntis hinausgehen, werden ausschließlich auf dem Gerät des Benutzers gespeichert; eine Synchronisierung dieser Daten mit den Untis-Systemen findet NICHT statt.

7. Welche Rechte stehen Ihnen hinsichtlich der Datenverarbeitung zu?

Wir möchten Sie darüber informieren, dass Sie das Recht haben,

- jederzeit Auskunft darüber zu verlangen, welche Daten von Ihnen bei uns verarbeitet werden. Das Recht auf Auskunft beinhaltet auch das Recht auf Erhalt einer Datenkopie, sofern dadurch Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden (siehe im Detail Art 15 DSGVO);
- die Berichtigung oder Vervollständigung Sie betreffender unrichtiger oder unvollständiger Daten zu verlangen (siehe im Detail Art 16 DSGVO);
- die Löschung Ihrer Daten zu verlangen (siehe im Detail Art 17 DSGVO). Das Recht auf Löschung besteht jedoch z.B. nicht, soweit die Verarbeitung zur Erfüllung einer rechtlichen oder vertraglichen Verpflichtung erforderlich ist;

- bei Vorliegen bestimmter Voraussetzungen die Einschränkung der Verarbeitung Ihrer Daten zu verlangen (siehe im Detail Art 18 DSGVO);
- gegen eine Verarbeitung Ihrer Daten, die zur Wahrung unserer berechtigten Interessen oder eines Dritten erforderlich sind, Widerspruch einzulegen. Im Fall eines Widerspruchs verarbeiten wir Ihre Daten nicht mehr, es sei denn, die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder wir weisen zwingende schutzwürdige Gründe für die Verarbeitung nach, die Ihre Interessen überwiegen. Widersprechen Sie einer Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten (siehe im Detail Art 21 DSGVO);
- die Übertragung der von Ihnen bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Das Recht auf Datenübertragbarkeit besteht jedoch nur, sofern die Verarbeitung auf Ihrer Einwilligung oder auf einem Vertrag beruht (siehe im Detail Art 20 DSGVO).

Zur Geltendmachung eines der oben genannten Rechte wenden Sie sich bitte an die jeweilige Bildungseinrichtung.

Sofern Ihr Anliegen eine Datenverarbeitung betrifft, die über jene hinausgeht, die Ihnen von Ihrer Bildungseinrichtung zur Verfügung gestellt wird, wenden Sie sich bitte – mit Nennung der jeweiligen Bildungseinrichtung – per E-Mail an [datenschutz\(at\)untis.at](mailto:datenschutz(at)untis.at) oder postalisch an Untis GmbH, Belvederegasse 11, A2000 Stockerau. Wir weisen darauf hin, dass eine Bearbeitung Ihrer Anfrage in der Regel nur in Zusammenarbeit mit der jeweiligen Bildungseinrichtung erfolgen kann.

Sollte es, trotz unserer Verpflichtung, Ihre Daten rechtmäßig zu verarbeiten, wider Erwarten zu einer Verletzung Ihres Rechtes auf rechtmäßige Verarbeitung Ihrer Daten kommen, setzen Sie sich bitte mit uns postalisch oder per E-Mail in Verbindung (Kontaktdaten siehe unten), damit wir von Ihren Bedenken erfahren und diese behandeln können. Sie haben aber auch das Recht, eine Beschwerde bei der Österreichischen Datenschutzbehörde oder bei einer anderen Datenschutz-Aufsichtsbehörde in der EU, insbesondere an Ihrem Aufenthalts- oder Arbeitsort, zu erheben.

Wir hoffen Ihnen mit dieser Information Klarheit darüber verschafft zu haben in welcher Form und für welche Zwecke wir Ihre Daten verarbeiten. Sollten Sie dennoch Fragen zur Verarbeitung Ihrer personenbezogenen Daten haben, können Sie sich gerne an uns wenden.

Datenschutzrechtliche Informationen - LMS Moodle

nach Art. 13 DSGVO

Wer ist verantwortlich für die Verarbeitung der Daten und wer kann Fragen zum Datenschutz beantworten?

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.de

Datenschutzbeauftragte/r:

Der Datenschutzbeauftragte/r des Verantwortlichen ist:
Datenschutzbeauftragte/r für die Schulen des Kreises Herford
Christian Meyer
Schulamt des Kreises Herford
Amtshausstraße 3
32051 Herford
Tel.: 05732/3779
DSB-Schulen-HF@kreis-herford.de

Allgemein

Durch die Nutzung der Lernplattform Moodle werden persönliche Daten über Sie gespeichert. Dazu gehören Ihr Vorname, Name, SchülerID, Emailadresse (sofern angegeben), sowie welche Kurse Sie nutzen und was Sie wann in diesen Kursen getan haben.

Leistungsergebnisse (Testergebnisse u.ä.) können bei Kursen, in denen dies eingerichtet ist, ebenfalls gespeichert werden. Diese Daten sind mit Ihrer Person verbunden. Es ist daher unsere Pflicht, Sie darüber zu informieren, dass diese Daten erfasst und verarbeitet werden und welche Rechte Sie diesbezüglich haben.

Andere Daten entstehen durch Bewertungen bei Tests und Aufgaben automatisch oder durch Kursbetreuer/Trainer. Zusätzlich werden Verbindungsdaten in Protokollen über Ihre Nutzung automatisch auf dem Server erstellt. Diese werden genutzt, um technische Probleme zu lösen und den technischen Betrieb zu gewährleisten. Zu den Verbindungsdaten gehören: IP-Adresse, Benutzerkonto (Login), Name der aufgerufenen Seite, Zugriffsstatus (http-Statuscode), Datum und Uhrzeit der Aktion.

An wen werden die Daten übermittelt?

Die Moodle-Instanz wird direkt vom August-Griese-Berufskolleg Löhne betrieben. Im Sinne des Datenschutzrechts findet somit keine Übermittlung statt.

Wir stellen sicher, dass intern nur die Personen Zugriff auf diese Informationen erhalten, die diesen Zugang unbedingt benötigen.

Zweck und Rechtsgrundlage

Die Lernplattform Moodle dient

- der Organisation und Durchführung und Verbesserung von Schulungen,
- dem Nachweis der Durchführung und des Abschlusses einer Schulung,

- der Erstellung von Zertifikaten nach erfolgreichem Abschluss.

Die erhobenen Daten werden zum Zweck der Verbesserung der Schulungsangebote ausgewertet.

Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Externe erhalten keinen Zugriff auf Ihre Daten.

Dauer der Speicherung oder Kriterien für die Dauer der Speicherung

Die Daten in Ihrem Nutzerprofil werden bis zur Löschung des Nutzerprofils gespeichert. Die Daten aus der Teilnahme am Kurs und eventuelle Testergebnisse werden bis zur Löschung des Kurses gespeichert.

Cookies

Mit der Nutzung von Moodle werden Cookies (= kleine Textdateien) im Webbrowser auf dem jeweiligen Computer lokal gespeichert. Der Zweck dieser Cookie ist zu gewährleisten, dass der Zugriff nach dem Login auf alle Seiten möglich ist und auf die richtige Seite zugegriffen wird. Nach dem Ausloggen bzw. Schließen Ihres Browsers werden Cookies automatisch gelöscht. Zudem dienen Cookies dem Zwecke der Bequemlichkeit. Es ist damit möglich, dass bei einem neuen Einloggen auf unserem Moodle-Server, der Username bereits automatisch in das Login-Formular eingetragen wird. Sie können diesen Cookie verbieten, müssen dann aber bei jedem Login Ihren Usernamen selbst wieder eingeben.

Rechte des Nutzers

Sie haben verschiedene Rechte gegenüber der verantwortlichen Stelle im Hinblick auf die über Sie gespeicherten Daten. Dazu gehören:

Auskunft durch den Verantwortlichen (s.o.) über die Daten, die über Sie gespeichert werden: Wenn Sie sich in der Plattform einloggen, können Sie diese Daten jederzeit selber einsehen.

In Ihrem Nutzerprofil haben Sie die Möglichkeit mit den Ansprechpartnern zu Datenschutzfragen Kontakt aufzunehmen und einen Bericht über gespeicherte Daten anzufragen.

Recht auf Berichtigung

Sofern inkorrekte Daten gespeichert werden, können Sie diese z.T. selber anpassen (selbst erfasste Profildaten) oder den Verantwortlichen auffordern dies zu tun. Der Verantwortliche wird der Aufforderung nachkommen, sofern die Berichtigung berechtigt und angemessen ist.

Recht auf Löschung

Sie haben ein Recht darauf, dass Daten gelöscht werden, die tatsächlich falsch sind oder für die der Verantwortliche keinen weiteren Zweck hat.

Ein Recht auf Löschung von Daten besteht nicht wenn der Verantwortliche verpflichtet ist, die Daten aus gesetzlichen Gründen noch vorzuhalten oder berechnete Interessen vorliegen.

Recht auf Einschränkung der Verarbeitung

Wir werden Ihren Zugang sperren, falls das Recht auf Verarbeitung oder der Inhalt strittig ist. Nach Aufklärung werden Daten korrigiert oder gelöscht. Der Verantwortliche wird sicherstellen, dass Daten im Falle der Einschränkung nur solchen Personen zugänglich sind, die die Daten unbedingt einsehen müssen. Dazu kann er sich der Mittel der Pseudonymisierung und der Anonymisierung bedienen.

Widerspruchsrecht

Sie können der weiteren Nutzung Ihrer Daten widersprechen. Dies kann nur in die Zukunft hinein wirksam werden. Das Widerspruchsrecht ist keine automatische Verpflichtung zur Löschung der Daten für den Verantwortlichen. Sofern der Verantwortliche Speicherpflichten aus anderen Gründen hat, wird er dies abwägen und Sie informieren.

Mit Eingang des Widerspruchs werden wir Ihren Nutzerzugang sperren. Der Widerspruch führt nicht dazu, dass Ihre Daten automatisch gelöscht werden.

Datenübertragbarkeit

Sie haben einen Anspruch, Daten, die von Ihnen selber erfasst wurden, in einem elektronischen Format zu erhalten. Das Recht ist beschränkt auf Daten, die nicht einem Betriebsgeheimnis unterliegen und daher nicht an andere Stellen übertragen werden dürfen oder die die Rechte anderer z.B. Urheberrecht betreffen.

Datenschutzrechtliche Informationen - Office 365

nach Art. 13 DSGVO

Mit diesem Schreiben informieren wir Sie über die zur Nutzung von Microsoft Office 365 inklusive der Clouddienste und Teams erforderliche Verarbeitung von personenbezogenen Daten.

Wer ist verantwortlich für die Verarbeitung der Daten und wer kann Fragen zum Datenschutz beantworten?

August-Griese-Berufskolleg Löhne
Die Schulleitung – vertr. durch Henning Tausch
Jahnstraße 54-68
32584 Löhne
Tel.: 05732/10840
E-Mail: agb@agb-loehne.de
Website: www.agb-loehne.de

Datenschutzbeauftragte/r:

Der Datenschutzbeauftragte/r des Verantwortlichen ist:
Datenschutzbeauftragte/r für die Schulen des Kreises Herford
Christian Meyer
Schulamt des Kreises Herford
Amtshausstraße 3
32051 Herford
Tel.: 05732/3779
DSB-Schulen-HF@kreis-herford.de

Zu welchem Zweck sollen meine Daten verarbeitet werden?

Die Datenspeicherung dient ausschließlich dem Zweck der unterrichtlichen Bereitstellung von Unterlagen. Die Unterlagen werden von den Schülern*innen individuell bearbeitet und können nur durch Freigabe des/der Schülers/Schülerin von anderen Personen eingesehen werden. Weiterhin ist die Verarbeitung erforderlich zur Nutzung von Microsoft Teams, einer Kommunikations- und Lernplattform mit der Möglichkeit zu Audio- und Videokonferenzen und zur Durchführung von Online-Unterrichtseinheiten in der Lerngruppe und zur individuellen Betreuung und Beratung in Kleingruppen oder Einzeltreffen zwischen Schüler/-in und Lehrkraft.

Auf welcher Rechtsgrundlage erfolgt die Verarbeitung?

Die Verarbeitung erfolgt auf der Grundlage Ihrer Einwilligung.

Welche personenbezogenen Daten werden bei der Nutzung von MS Office 365 inklusive MS Teams verarbeitet?

Verarbeitet werden Daten zur Erstellung eines Nutzerkontos (E-Mail Adresse, Passwort, Schulzugehörigkeit, Zugehörigkeit zu Teams, Rollen und Rechte zur Anzeige eines Nutzerstatus und von Lesebestätigungen (Chat), erstellte Chat-Nachrichten, Sprachnotizen, Bild- und Tondaten in Video- und Audiokonferenzen, Inhalte von Bildschirmfreigaben, durch Hochladen geteilte Dateien, erstellte Kalendereinträge, Status von Aufgaben (zugewiesen, abgegeben, Fälligkeit, Rückmeldung), in Word, Excel, PowerPoint und OneNote erstellte und bearbeitete Inhalte, Eingaben bei Umfragen, technische Nutzungsdaten zur Bereitstellung der

Funktionalitäten und Sicherheit von MS Teams und in Teams integrierte Funktionen). Eine Speicherung der Bild- und Tondaten von Videokonferenzen durch die Schule erfolgt nicht.

Die aktuelle Datenschutzerklärung von Microsoft kann hier eingesehen werden:

<https://privacv.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 freigeben,*
- 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.”*

Wer ist für die Datensicherung verantwortlich?

Weder die Schule noch Microsoft ist für die Ausfalldatensicherung der in der Cloud liegenden Daten verantwortlich. Der/Die Benutzerin hat somit selbst sicherzustellen (z.B. durch regelmäßige Backups), dass im Falle eines Systemausfalls im Datenzentrum, keine für den/die Benutzerin relevanten Daten verloren gehen.

Was tut die Schule zum Schutz meiner personenbezogenen Daten in MS Teams?

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 MS Teams und der Cloud mit der größtmöglichen Sicherheit abläuft. Wir haben das System so voreingestellt, dass durch das Handeln und Fehler der Nutzerinnen selbst möglichst wenige Risiken entstehen können. Ganz zentral ist die Schulung der Nutzerinnen für einen sicheren und verantwortungsvollen Umgang mit den Werkzeugen in MS Teams. Vor Erteilung des Zugangs findet eine Grundschulung statt. Diese wird durch eine jährliche Belehrung und die Nutzungsvereinbarung/Dienstanweisung ergänzt.

Wer hat Zugriff auf meine personenbezogenen Daten?

Auf alle in die Cloud und in Teams durch Nutzer eingestellten Dateien, Inhalte und Kommentare haben jeweils die Personen Zugriff, mit denen sie geteilt werden. Das können Einzelpersonen sein oder Mitglieder eines Teams oder Channels in einem Team. Lehrkräfte haben Zugriff auf innerhalb von gestellten Aufgaben vorgenommene Bearbeitungen und erstellte Inhalte. Alle Teilnehmer einer Videokonferenz haben Zugriff im Sinne von Sehen, Hören und Lesen auf Inhalte der Videokonferenz, Chats, geteilte Dateien und Bildschirmfreigaben. In einem Chat haben alle Teilnehmer Zugriff auf eingegebene Inhalte und geteilte Dateien. Der Anbieter hat Zugriff auf die bei der Nutzung von Teams anfallenden Daten soweit dieses zur Erfüllung seiner

Verpflichtung im Rahmen des mit der Schule abgeschlossenen Vertrags zur Auftragsverarbeitung erforderlich ist.

An wen werden die Daten übermittelt?

Wir nutzen Microsoft Office 365 und MS Teams im Rahmen eines Vertrags zur Auftragsverarbeitung. Microsoft verarbeitet deine personenbezogenen Daten ausschließlich in unserem Auftrag. Demnach darf Microsoft sie nur entsprechend unserer Weisungen und für unsere Zwecke und nicht für eigene Zwecke nutzen, also weder für Werbung und auch nicht, um sie an Dritte weitergeben. Im Sinne des Datenschutzrechts findet somit keine Übermittlung statt.

Wie lange werden meine Daten gespeichert?

Die Speicherung von Daten, welche zur Bereitstellung des Nutzerkontos verarbeitet werden, sowie erstellte und geteilte Inhalte, Kommentare, Chat-Nachrichten, Sprachnachrichten, zugewiesene, bearbeitete und abgegebene Inhalte und Kalendereinträge, endet, sobald der/die Nutzer/-in die Schule verlassen hat, seine/ihre Einwilligung ganz oder in Teilen widerruft oder einer Verarbeitung widerspricht. Die Löschung erfolgt dann innerhalb von vier Wochen nach Verlassen der Schule. Die Löschung aus den Systemen von Microsoft ist vom Zeitpunkt der Löschung eines Kontos oder von Inhalten durch die Schule nach 90 Tagen abgeschlossen. Selbiger Zeitraum gilt auch für die Löschung von Dateien durch den Nutzer selbst. Ton- und Bilddaten von Video- und Audiokonferenzen werden von der Schule nicht aufgezeichnet und gespeichert. Inhalte in von anderen geteilten Dateien, bearbeitete und abgegebene Aufgaben und Nachrichten in Gruppenchats werden gespeichert, solange ein Team besteht. Teams für Klassen- und Lerngruppen werden spätestens 5 Jahre nach Ende der Schulzeit der betroffenen Schüler/-innen samt ihren von Schülern/Schülerinnen erstellten, geteilten und bearbeiteten Inhalten und Chats gelöscht. Inhalte von Chats bestehen solange das Konto des anderen Nutzers besteht.

Zusätzliche Informationen

Wo werden meine personenbezogenen Daten verarbeitet?

Alle Daten, die unter Verwendung des von der Schule generierten Logins in der Microsoft-Cloud gespeichert werden, liegen in Datenzentren innerhalb der Europäischen Union und unterliegen somit den gültigen Datenschutzgesetzen der EU. Die für die Kontoerstellung verwendeten oder in den Systemen von Microsoft gespeicherten Daten werden nicht an Dritte weitergegeben. Der Zugriff auf die Daten ist nur dem/der Benutzerin unter Verwendung eines von ihm/ihr selbst erstellten, sicheren Kennworts möglich. Das Login/Authentifizierung zu den Office 365-Clouddiensten geschieht durch Rechenzentren, die in den USA liegen.

„Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ist ein US-amerikanisches Gesetz. Es verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt. Dem von der Herausgabeverpflichtung betroffenen Unternehmen steht jedoch nach dem Gesetz im Einzelfall ein Widerspruchsrecht gegen die Anordnung zur Herausgabe von Daten zu, wenn der Eigentümer der Daten kein US-Bürger ist, nicht in den USA lebt und das Unternehmen durch die Herausgabe der Daten gegen ausländisches Recht (in Europa zum Beispiel die DSGVO) verstoßen würde.“

Quelle: https://de.wikipedia.org/wiki/CLOUD_Act

Wie sicher ist Microsoft Teams und die Cloud?

Die Plattform genügt allen gängigen Sicherheitsstandards für Cloud Plattformen.