

Realschule Rees

Westring 4, 46459 Rees



Nutzungsvereinbarung pädagogisches Netz und Microsoft 365 sowie datenschutzrechtliche Informationen gemäß Art. 13 DS-GVO:

Die im folgenden Text verwendete männliche Form bezieht sich immer zugleich auf weibliche, männliche und diverse Personen. Auf eine Doppelnennung und gegenderte Bezeichnungen wird zugunsten einer besseren Lesbarkeit verzichtet.

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhältst du / erhalten Sie Zugang zum pädagogischen Netzwerk unserer Schule (inklusive eines Zugangs zum Internet) und zu unseren Arbeits- und Kommunikationsplattformen Relution, WebUntis, LogoDidact (im Folgenden „pädagogisches Netz“) sowie Microsoft 365 Education inklusive Microsoft Teams (im Folgenden „Microsoft 365“). Den Zugang zum pädagogischen Netz und Microsoft 365 stellen wir dir / Ihnen auch außerhalb des Unterrichts **zur schulischen Nutzung** zur Verfügung. Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, den Plattformen 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 für eine verantwortungsvolle Nutzung ab. Ihre Annahme bzw. die Einwilligung sind Voraussetzung für die Erteilung eines Nutzerzugangs.

Nutzungsvereinbarung

Geltungsbereich

Die Nutzungsvereinbarung gilt für Schülerinnen und Schüler sowie Lehrkräfte, nachfolgend „Benutzer“ genannt, welche das von der Schule bereitgestellte pädagogische Netzwerk einschließlich der Zugänge zu Relution, WebUntis, LogoDidact und zum Internet sowie Microsoft 365 zur elektronischen Datenverarbeitung nutzen.

Laufzeit

Dem Benutzer werden innerhalb seiner Dienstzeit / Schulzeit ein Benutzerkonto im pädagogischen Netz sowie eine Microsoft 365 Education Lizenz zur Verfügung gestellt. Das Benutzerkonto wird deaktiviert und gelöscht sowie die Zuweisung der Microsoft 365 Education Lizenz aufgehoben, wenn der Benutzer die Schule verlässt.

Die Bereitstellung der Microsoft-Lizenzen erfolgt freiwillig. Es besteht kein Anspruch auf diese Lizenz. Die Schule behält sich das Recht vor, die den Benutzern zur Verfügung gestellten Microsoft 365 Education Lizenzen jederzeit zu entziehen. Ebenso behält sich die Schule das Recht vor, die Nutzung einzelner Arbeits- und Kommunikationsplattformen im Rahmen der Weiterentwicklung des Medienkonzepts zu beenden.

Umfang

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

- Zugang zum pädagogischen Netz der Schule mit einem persönlichen Benutzerkonto.
- WLAN-Zugang zum pädagogischen Netz mit einem personalisierten Leihgerät.
- Zugang zu Microsoft 365 mit
 - einer schulischen E-Mail-Adresse (für Schülerinnen und Schüler teilweise nur für schulintern nutzbar)
 - Online-Speicherplatz auf Microsoft OneDrive
 - Microsoft Office 365 (u.a. Teams, Word, Excel, PowerPoint, OneNote)
 - Minecraft Education
 - der Möglichkeit, Microsoft 365 auf bis zu 5 Geräten parallel zu nutzen.

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 und den anderen Anbietern der Arbeits- und Kommunikationsplattformen wurde zur Nutzung ein Vertrag abgeschlossen,

Nutzungsvereinbarung pädagogisches Netz und Microsoft 365
sowie datenschutzrechtliche Informationen gemäß Art. 13 DS-GVO:

welcher gewährleistet, dass personenbezogene Daten von Benutzern nur entsprechend der Vertragsbestimmungen verarbeitet werden (Vertrag zur Auftragsdatenverarbeitung). Bei Microsoft wird das Online Service Terms (OST) genannt, wozu auch das Data Processing Addendum (DPA) gehört. Bestandteil des DPA sind die sogenannten Standardvertragsklauseln.

Microsoft verpflichtet sich, die personenbezogenen Daten von Benutzern in Microsoft 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 Microsoft 365 auf das maximal erforderliche Maß, das Recht auf informationelle Selbstbestimmung der Benutzer bestmöglich zu schützen.

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

An erster Stelle gilt dies für die Nutzung von personenbezogenen Daten in der Cloud von Microsoft 365. Es gilt jedoch auch für das pädagogische Netz der Schule.

Personenbezogene Daten gehören grundsätzlich nicht in die Microsoft Cloud (z.B. Microsoft OneDrive), weder die eigenen noch die von anderen. Jeder Benutzer hat dafür zu sorgen, dass die Sicherheit und der Schutz von personenbezogenen Daten nicht durch leichtfertiges, fahrlässiges oder vorsätzliches Handeln gefährdet werden.

Soll mit personenbezogenen Daten gearbeitet werden (z.B. Lebenslauf), muss dies offline im pädagogischen Netz erfolgen. Innerhalb des pädagogischen Netzes der Schule können, außerhalb von Microsoft 365, personenbezogene Daten genutzt und gespeichert werden, solange dies sparsam und zu Unterrichtszwecken erfolgt. Sollten ihr / Sollten Sie sich nicht sicher sein, ob der Speicherort geeignet ist, ist auf die Speicherung der Daten zu verzichten.

Verantwortungsvolles und sicheres Handeln bedeutet:

Zugangsdaten

- Passwörter für das pädagogische Netz und Microsoft 365 müssen sicher sein und dürfen nicht leicht zu erraten sein. Dabei können die Anforderungen an die Passwortkomplexität je nach Anwendung unterschiedlich sein. Eine Checkliste zur Erstellung von sicheren Passwörtern hat das BSI (Bundesamt für Sicherheit in der Informationstechnik > <https://www.bsi.bund.de>) bereitgestellt. ¹
- Passwörter für Microsoft 365 und das pädagogische Netz dürfen nicht für andere Zugänge im privaten Bereich genutzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten oder im Webbrowser gespeichert werden. Die Auto-Speichern-Funktion für Passwörter darf nicht genutzt werden.
- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum pädagogischen Netz und zum persönlichen Microsoft 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 dies nicht möglich, ist der in der Schule zuständige Mitarbeiter (siehe Organigramm der Schule) zu informieren.
- Sollte der Benutzer Kenntnis von fremden Zugangsdaten erlangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Der Benutzer ist jedoch verpflichtet, den Eigentümer der Zugangsdaten oder den in der Schule zuständige Mitarbeiter (siehe Organigramm der Schule) zu informieren.
- Nach Beendigung der Arbeitssitzung an einem schulischen Rechner bzw. Mobilgerät, bzw. spätestens am Ende der Unterrichtsstunde, meldet sich der Benutzer von Microsoft 365 und dem pädagogischen Netz ab (ausloggen).

¹ „Sichere Passwörter erstellen“ https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Personenbezogene Daten

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

E-Mail und Kalender

- Die Nutzung des schulischen E-Mail-Kontos ist nur für schulische Zwecke zulässig.
- Wie bei den anderen Komponenten von Microsoft 365 ist auch beim Versand von E-Mails die Nutzung von personenbezogenen Daten zu minimieren.
- Verdächtige E-Mails aus unbekannten Quellen – mit Links oder ausführbaren Dateien – dürfen nicht geöffnet werden. Ausführbare Dateien sind an der Dateiendung erkennbar (u.a. .com, .exe, .bat, .cmd, .msc, .hta, .pif).

Kopplung mit privaten Konten oder anderen Diensten

- Bei der Nutzung von Office 365 auf privaten Geräten ist darauf zu achten, dass keine Synchronisation privater Daten mit Microsoft OneDrive erfolgt.
- Zur Wahrung des Schutzes und der Sicherheit der eigenen personenbezogenen Daten ist es nicht erlaubt, das schulische Microsoft 365 Konto mit anderen privaten Konten von Microsoft oder anderen Anbietern zu verknüpfen.
- Eine Nutzung des schulischen Microsoft 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 Microsoft 365 sind die geltenden Bestimmungen des Urheberrechts zu beachten.
- Fremde Inhalte (Texte, Fotos, Videos, Audio und andere Materialien) dürfen nur mit schriftlicher Genehmigung des Urhebers veröffentlicht werden. Dies gilt auch für digitalisierte Inhalte. Dazu gehören eingescannte oder abfotografierte Texte und Bilder. Bei vorliegender Genehmigung ist bei Veröffentlichungen auf einer eigenen Website 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“² im pädagogischen Netz oder in Microsoft 365 in digitalem Format eingestellt wurden, dürfen vom Benutzer nicht an andere Personen außerhalb der Klassen- oder Kursgruppe weitergegeben werden.
- Bei den digitalen Inhalten von Lehrmittelverlagen, die von der Schule über das pädagogische Netz oder Microsoft 365 zur Verfügung gestellt werden, muss das Urheberrecht beachtet werden.
- Die Urheberrechte an Inhalten, die Benutzer eigenständig erstellt haben, bleiben durch eine Ablage oder Bereitstellung im pädagogischen Netz oder in Microsoft 365 unberührt.

Unzulässige Inhalte und Handlungen

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

- Die geltenden Rechtsvorschriften – auch innerschulischer Art – sind einzuhalten. Dazu gehören Urheber-, Jugendschutz-, Datenschutz- und Strafrecht sowie die Schulordnung.
- Es ist verboten, pornografische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder diffamierende Inhalte über das pädagogische Netz und Microsoft 365 abzurufen, zu speichern oder zu verbreiten.
- Die Verbreitung und das Versenden von belästigenden, verleumderischen oder bedrohenden Inhalten ist unzulässig.
- Die E-Mail-Funktion von Microsoft 365 darf nicht für die Versendung von Massen-Nachrichten (Spam) und / oder anderen Formen unzulässiger Werbung genutzt werden.

² „Schulbuchkopie“ <http://www.schulbuchkopie.de/> Abgerufen 17. Okt. 2024

Nutzungsvereinbarung pädagogisches Netz und Microsoft 365
sowie datenschutzrechtliche Informationen gemäß Art. 13 DS-GVO:

Technische Unterstützung:

- Alle Benutzer tragen dafür Verantwortung, die Datensicherheit im pädagogischen Netz zu gewährleisten. Netzwerkressourcen sind nur so zu nutzen, dass diese Datensicherheit nicht gefährdet wird. Dies bedeutet konkret: Vorgegebene Sicherheitseinstellungen (z.B. Firewalls) und Virenschutzprogramme dürfen nicht deaktiviert oder umgangen werden. In Zweifelsfällen sind die Ansprechpartner in der Schule um Rat zu fragen.
- Erster Ansprechpartner in Angelegenheiten der Informationstechnik (Fragen, Störungen oder Unklarheiten usw.) sind die Medienbeauftragten an den Schulen. Informationen zur Kontaktaufnahme werden an den Schulen kommuniziert.
- Unterstützt wird die Schule in diesem Bereich vom IT-Service des Schulträgers, der Stadt Rees. Die Stadt Rees verarbeitet personenbezogene Daten im Auftrag der Schule.

Zu widerhandlungen

Im Falle von Verstößen gegen diese Nutzungsordnung behält sich die Schulleitung das Recht vor, den Zugang zu einzelnen oder allen Bereichen innerhalb des pädagogischen Netzes und von Microsoft 365 zu sperren. Davon unberührt behält sich die Schulleitung weitere dienstrechtliche Maßnahmen (Lehrkräfte) oder Ordnungsmaßnahmen (Schüler) sowie die Prüfung einer Anzeige bei der Polizei vor.

Datenschutzrechtliche Informationen nach Art. 13 DS-GVO

Zur Erfüllung des Bildungs- und Erziehungsauftrags verarbeiten wir personenbezogene Daten in analoger und digitaler Form, in Lehr- und Lernsystemen sowie Arbeits- und Kommunikationsplattformen. Darüber möchten wir Sie/Euch im Folgenden informieren.

Datenverarbeitende Stelle

Realschule Rees
Westring 4, 46459 Rees

Schulischer Datenschutzbeauftragter

Schulleitung: Hr. Wenning
Tel.: +49 2851 9799344
E-Mail: realschule@stadt-rees.de

Zwecke der Verarbeitung personenbezogener Daten

Die Verarbeitung von personenbezogenen Daten erfolgt zu einer Vielzahl von Zwecken, die mit der Organisation des Schulalltags, schulinternen Verwaltungstätigkeiten, der Gestaltung von Lehr- und Lernprozessen sowie der internen und externen Kommunikation zu tun haben. An unserer Schule geht es dabei um die folgenden **Verarbeitungszwecke**:

- Durchführung von Unterricht,
- Verwaltung von Schülerdaten und Noten, Durchführung von Prüfungen sowie Zeugniserstellung,
- Unterrichtsplanung, -durchführung und Dokumentation,
- Durchführung des Bildungsgangs ggf. mit Kurswahl und Überprüfung der Zulassungsvoraussetzungen, sowie der Erteilung von Berechtigungen,
- Evaluation, Qualitätsentwicklung und Schulstatistik,
- Kommunikation mit den Erziehungsberechtigten, Dokumentation von Erziehungs- und Ordnungsmaßnahmen,
- Diagnostik / Erstellung von Förderempfehlungen/ individuellen Förderplänen,
- Erstellung von Fördergutachten (AO-SF Verfahren),
- Schulpflichtüberwachung,
- Öffentlichkeitsarbeit,
- Organisation des Schülerspezialverkehrs,
- Praktikumsverwaltung

Personenbezogene Daten der Benutzer des pädagogischen Netzwerks unserer Schule (inklusive eines Zugangs zum Internet) sowie unserer Arbeits- und Kommunikationsplattformen Relution, WebUntis und LogoDidact (im Folgenden „pädagogisches Netz“) sowie Microsoft 365 Education inklusive Microsoft Teams (im Folgenden „Microsoft 365“) werden verarbeitet, 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. Bei der Nutzung von Microsoft Teams werden personenbezogene Daten verarbeitet, um Online-Unterrichtseinheiten in der Lerngruppe sowie individuelle Betreuung und Beratung durchführen zu können.

Rechtsgrundlage der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten von Schülern, Eltern und Lehrkräften, bzw. verpflichteten Personen erfolgt in der Schule überwiegend auf der Grundlage des **Schulgesetzes von Nordrhein-Westfalen** in Verbindung mit **Art. 6 Abs. 1 lit e) DS-GVO**.

Personenbezogene Daten, die nicht unter diese Regelungen fallen, erheben und verarbeiten wir nur mit Ihrer informierten und freiwilligen Einwilligung. Dazu gehören beispielsweise Notfallinformationen, Ihre Telefonnummer am Arbeitsplatz, Ihre private sowie berufliche E-Mail-Adresse, Aufnahmen von Fotos, Videos und Audio zur unterrichtlichen Nutzung und Veröffentlichungen auf der Schulhomepage und in der Presse, sowie Daten, die bei der Nutzung von nicht auf der Grundlage von § 120 Abs. 5 Satz 2 verpflichtend eingeführten Arbeits- und Kommunikationsplattformen und Lehr- und Lernplattformen anfallen.

Kategorien von personenbezogenen Daten

	Pädagogisches Netz	Relution (MDM)	WebUntis	LogoDidact	Microsoft 365	Apple School Manager
Anmeldedaten (Nutzerkennung, Passwort, Passwordinweis)	X	X	X	X	X	X
Nutzerdaten (Zuordnung zu Gruppen, Rechte und Rollen)	X	X	X	X	X	X
Nutzerinhalte (erzeugte Dateien und Inhalte, Versionen von Dateien, Interaktionen, Profildaten)	X	X	X	X	X	X
Kommunikationsdaten (Audio- und Videodateien, Daten in Chats, Konferenzen und Bildschirmfreigaben)			X	X	X	X
Technische Daten (Datum, Zeit, Traffic, IP-Adressen z.B. genutzter Dienste oder aufgesuchter Seiten)	X	X	X	X	X	X
Geräteidentifikationsdaten (Gerätenamen, MAC-Adresse)	X	X			X	X
Positionsdaten		X			X	X

Wichtiger Hinweis: Positionsdaten können nicht unbemerkt ausgelesen werden.

Kategorien von Empfängern

	Pädagogisches Netz	Relution (MDM)	WebUntis	LogoDidact	Microsoft 365	Apple School Manager
Intern						

Schüler (eigene Daten und Daten von Mitschülern entsprechend Freigabe von Lehrkräften und Mitschülern; Namenslisten besuchter Klassen / Kurse)	X	X	X	X	X	X
Lehrkräfte (eigene Daten und Daten von Schülern und Lehrkräften entsprechend ihrer Funktion und Freigaben durch die Personen selbst)	X	X	X	X	X	X
Schulische Administratoren / Medienbeauftragte (alle technischen und öffentlichen, eingeschränkte administrative Rechte)	X	X	X	X	X	X
Schulleitung (alle technischen und öffentlichen Daten, ohne administrative Rechte; 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)	X	X	X	X	X	X
Extern						
Eltern (bei Freigabe durch Schüler; Stunden- und Vertretungspläne des Kindes)			X	X	X	X
Administratoren des Schulträgers (alle Daten aller Personen, soweit für administrative Zwecke erforderlich, auf Weisung der Schulleitung)	X	X	X	X	X	X
Dienstleister / Administratoren des Auftragverarbeiters (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich, auf Weisung der Schulleitung)	X	X	X	X	X	X
Ermittlungsbehörden (alle Daten betroffener Nutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)	X	X	X	X	X	X
US-Ermittlungsbehörden (haben Zugriff nach US-amerikanischem Recht; weitere Informationen siehe unten)					X	X
Betroffene (Auskunftsrecht nach Art. 15 DS-GVO)	X	X	X	X	X	X

Um die Administration der Plattformen sicherzustellen, hat die Schule die Stadt Rees mit der weisungsgebundenen Verarbeitung von personenbezogenen Daten beauftragt (Auftragsdatenverarbeitung). Die Stadt Rees hat ihrerseits das Kommunale Rechenzentrum Niederrhein (nachfolgend KRZN); die Firma SBE network solutions GmbH (LogoDidact und Relution) und Microsoft (Microsoft 365) mit der Verarbeitung von personenbezogenen Daten aus der Schule beauftragt. Das KRZN, SBE network solutions GmbH und Microsoft sind Unterauftragsnehmer. Über die Auftragskette hinweg bleibt die Schule verantwortlich gemäß Art. 4 Nr. 7 DS-GVO.

Die Schule hat direkt einen Auftragsverarbeitungsvertrag mit der Untis GmbH sowie deren Partner für Nordrhein-Westfalen, der PEDAV das Softwarehaus für Schulen GmbH & Co. KG, abgeschlossen.

Übermittlung von personenbezogenen Daten

Wir übermitteln personenbezogene Daten regelmäßig oder bei Bedarf an Stellen außerhalb der Schule. Dazu gehört das Schulministerium (IT.NRW) für statistische Auswertung und Planung. Im Rahmen der Schulgesundheitspflege ist es die **untere Gesundheitsbehörde**, die **aufnehmende Schule** bei Schulwechsel, **Erziehungsberechtigte** sowie **Schülerinnen und Schüler** bei Mitteilungen und Zeugnissen. Außerdem das **Jugendamt**, **Landesjugendamt**, die **Schulaufsicht** und der **Schulträger**, soweit dies zur Erfüllung der Aufgaben der Schule erforderlich ist. Innerhalb der Schule sind die **Lehrkräfte** Empfänger der Daten. Nach Ablauf der Aufbewahrungsfrist werden ein Teil der Daten vom örtlichen **Archiv** übernommen.

Zur Öffentlichkeitsarbeit übermitteln wir gelegentlich personenbezogene Daten an die **lokale Presse**.

Bei einem Schulwechsel erhalten wir von der **abgebenden Schule** in Kopie personenbezogene Daten, die für die weitere Schulausbildung von Bedeutung sind. Das sind Individualdaten und gegebenenfalls Daten über sonderpädagogischen Förderbedarf, gesundheitliche Beeinträchtigungen und/oder körperliche Behinderungen, soweit dies für eine besondere schulische Betreuung der Betroffenen erforderlich ist. Außerdem erhalten wir Informationen zur Überwachung der Schulpflicht und eine Zweitschrift des letzten Zeugnisses oder Halbjahreszeugnisses. Bei weiterführenden Schulen: Von der abgebenden Grundschule erhalten wir das Ergebnis der Grundschulempfehlung.

Löschfristen

Wie lange die von uns verarbeiteten personenbezogenen Daten gespeichert werden, gibt das Schulgesetz NRW vor. Die nachfolgende Tabelle gibt einen Überblick über die Dauer der Aufbewahrung.

Nr.	Datenarten	Aufbewahrungszeit / Löschfrist
1.	Zweitschriften von Abgangs- und Abschlusszeugnissen	50 Jahre
2.	Schülerstammbblätter	20 Jahre
3.	Zeugnislisten, Zeugnisdurchschriften, (soweit es sich nicht um Abgangs- und Abschlusszeugnisse handelt), Unterlagen über die Klassenführung (Klassenbuch, Kursbuch), Akten über Schülerprüfungen	10 Jahre
4.	alle übrigen Daten	5 Jahre
5.	von Lehrkräften mit Genehmigung der Schulleitung auf privaten Computern verarbeitete personenbezogene Daten	1 Jahr (nach Abgabe des Schülers, ab Ende des Kalenderjahres)
6.	Führen einer Schulchronik: 1. Name, Vorname, Jahr der Beendigung des Schulverhältnisses	unbegrenzte Speicherung

Pädagogisches Netz

Zugangs- und Nutzungsdaten bleiben bestehen, solange der Benutzer Mitglied im pädagogischen Netz ist. Logdaten von Anmeldungen am pädagogischen Netz und Endgeräten sowie von Internetzugriffen aus dem pädagogischen Netz werden automatisch nach 14 Tagen gelöscht. Nach Ende der Schulzugehörigkeit werden sämtliche Zugangsdaten sowie das Nutzerverzeichnis 90 Tage aufbewahrt und danach gelöscht. Bis dahin ist es für den Benutzer möglich, die Inhalte des persönlichen Verzeichnisses eigenständig zu sichern.

Relution (MDM)

Die Benutzerdaten werden so lange gespeichert, wie die Benutzer ein schulisches, mobiles Endgerät nutzen. Nach Beendigung der Nutzung werden sie spätestens mit Ende der Schulzugehörigkeit gelöscht. Die Kontodaten des Benutzers werden innerhalb von 90 Tagen nach Beendigung der Nutzung endgültig gelöscht. Unterrichtsdaten werden am Schuljahresende gelöscht. Daten im Zusammenhang mit der Erstellung und Verwaltung von Benutzerkonten für die Nutzung, 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 Profildaten und Freigaben eigenständig zu löschen.

WebUntis

Die Anmelde- und Nutzerdaten werden solange gespeichert, wie diese WebUntis nutzen. Sie werden spätestens mit dem Ende der Schulzugehörigkeit gelöscht. Nach Beendigung der Nutzung werden die Kontodaten des Benutzers innerhalb von 90 Tagen endgültig aus WebUntis gelöscht. Die Untis GmbH / PEDAV 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 und Verwaltung von Benutzerkonten für die Nutzung, 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 Profildaten und Freigaben eigenständig zu löschen.

LogoDidact

Hinsichtlich der im Auftrag verarbeiteten Daten gilt die im Auftragsverarbeitungsvertrag festgelegte Löschung: Die Daten beim Auftragnehmer werden nach Artikel 28 Abs. 3 Buchstabe e spätestens mit der Beendigung der Auftragsverarbeitung gelöscht. Datensicherungen können noch bis zu 6 Monate über das Vertragsende hinaus Daten enthalten, die gelöscht wurden.

Die Verarbeitung nutzungsbezogener Daten (Pädagogische Prozessdaten; schülerbezogene Ergebnisse von Tests, bearbeitete Aufgaben usw.) ist für die Erfüllung des Zwecks der unterrichtlichen Nutzung erforderlich. Die Daten dieser Kategorie werden in der Regel am Ende jedes Schuljahres gelöscht. In begründeten Ausnahmefällen ist eine Verlängerung der Löschfrist zur schuljahresübergreifenden Verwendung von Dateien möglich. Darüber entscheidet letztendlich die Schulleitung und weist die zuständige Administration entsprechend an. Ausnahmefälle sind dementsprechend frühzeitig bei der Schulleitung zu melden.

Microsoft 365

Wird die Zuweisung der Microsoft 365 Lizenzen aufgehoben – in der Regel mit dem Ende der Schulzugehörigkeit –, 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 lang 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.³
- Benutzer müssen ihre Daten vorher eigenständig sichern.

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 samt ihren von Schülern erstellten, geteilten und bearbeiteten Inhalten und Chats gelöscht. Inhalte von Chats bestehen, solange das Konto des anderen Nutzers besteht.

Betroffenenrechte

Für personenbezogene Daten, deren Verarbeitung auf Ihrer **Einwilligung** beruht, kann diese Einwilligung für die Zukunft jederzeit widerrufen werden. Dabei kann der Widerruf auch nur auf einen Teil der Daten bezogen sein. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Im Falle eines Widerrufs werden entsprechende Daten zukünftig nicht mehr von uns genutzt und unverzüglich aus unserem Datenbestand gelöscht. Sollte die Einwilligung nicht widerrufen werden, gelten die oben genannten Löschfristen weiterhin.

Gegenüber der Schule besteht ein Recht auf **Auskunft** über Ihre personenbezogenen Daten. Ferner haben Sie grundsätzlich 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.

³ Siehe Verwalten von Lizenzen und Inhalten für Abschlussstudenten in Microsoft 365 Education (<https://support.microsoft.com/de-de/topic/verwalten-von-lizenzen-und-inhalten-f%C3%BCr-abschlussstudenten-in-microsoft-365-education-ba3142c7-fa7d-46d2-9efd-f1ee751cd400?omkt=de-de>)
Abgerufen 17. Okt. 2024

Zusätzliche Informationen zur Nutzung von Microsoft 365

Datenschutz bei Verarbeitung von personenbezogenen Daten in den USA

Die Verarbeitung von personenbezogenen Daten in Microsoft 365 und angebundenen Produkten erfolgt überwiegend auf Servern mit Standort im Europäischen Wirtschaftsraum (EWR). Die Verarbeitung dieser Daten unterliegt den strengen Regelungen der DS-GVO. Es ist möglich, dass sogenannte Telemetriedaten – eine Art Diagnosedaten – in den USA verarbeitet werden. Dabei geht es also weniger um Inhalte von Chats, Videokonferenzen, Terminen, gestellten Aufgaben, Nutzerkonten und Teamzugehörigkeiten, sondern um Daten, welche dazu dienen, die Sicherheit und Funktion der Plattform zu gewährleisten und zu verbessern. Die USA sind ein Drittland gemäß DS-GVO. Für Drittländer kann die DS-GVO kein angemessenes Schutzniveau für die Verarbeitung von personenbezogenen Daten sicherstellen. Die aktuelle Rechtslage zum Datenschutz im Drittland ist individuell zu überprüfen.

Im Rahmen des CLOUD-Act haben US-Ermittlungsbehörden umfassende Zugriffsrechte auf Daten von US-Unternehmen, einschließlich deren Daten in der EU. Dort werden die meisten Daten gespeichert, die bei einer Nutzung von Microsoft 365 und Teams in deutschen Schulen anfallen. Nutzer erfahren davon nichts und haben auch keine rechtlichen Möglichkeiten, sich dagegen zu wehren. 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 bis Dezember 2019 insgesamt 3.310 Anfragen von Ermittlungsbehörden an. Davon kamen die meisten aus Deutschland. Die Risiken, die durch diese Zugriffsmöglichkeiten von US-Ermittlungsbehörden entstehen, dürften eher gering sein.

In der Vergangenheit gab es bereits Datenschutzabkommen zwischen der EU und den USA, um eine sichere Rechtsgrundlage für einen transatlantischen Datentransfer zu schaffen und individuelle Prüfungen der Situation überflüssig zu machen. Diese Abkommen hielten einer gerichtlichen Überprüfung allerdings bisher nicht stand. Bereits 2015 klagte der Österreicher Max Schrems erfolgreich vor dem Europäischen Gerichtshof gegen das Safe-Harbor-Abkommen (Schrems I). Zuletzt erklärte der Europäische Gerichtshof (EuGH) mit seinem Urteil vom 16. Juli 2020 den Angemessenheitsbeschluss der Europäischen Kommission zum Privacy Shield-Abkommen für ungültig (Schrems II). Bei beiden Klagen ging es im Kern um die beschriebenen Kritikpunkte im Rahmen des CLOUD-Act.

Um Rechtssicherheit bezüglich Datentransfers zwischen den USA und der EU herzustellen, haben die USA mit der EU nun einen neuen Datenschutzrahmen (EU-US Data Privacy Framework) vereinbart. Gleichzeitig soll die Executive Order 14086 "Enhancing Safeguards for United States Signals Intelligence Activities", welche US-Präsident Biden bereits am 07. Oktober 2022 erließ, die Zugriffsrechte der Behörden eindämmen und EU-Bürgern geeignete Rechtsmittel zur Verfügung stellen. Erste Anlaufstelle für EU-Bürger soll nun der Civil Liberty Protection Officer sein, der für die Einhaltung von Grund- und Datenschutzrechten bei den US-Nachrichtendiensten zuständig ist. Dessen Entscheidungen können nun vor einem gänzlich neu eingerichteten, unabhängigen Gericht angefochten werden, dem Data Protection Review Court. Damit geht man auf die beiden wesentlichen Kritikpunkte an den USA als Datenempfänger ein. Mit dem Erlass des Angemessenheitsbeschlusses für das EU-US Data Privacy Framework vom 10. Juli 2023 attestiert die Europäische Kommission zertifizierten Unternehmen in den USA demnach auch ein angemessenes Schutzniveau für die Verarbeitung von personenbezogenen Daten, die innerhalb dieses Rahmens übertragen werden. Microsoft hat sich bereits gemäß diesem Datenschutzrahmen zertifizieren lassen.

Die EU und die USA sind zuversichtlich damit einen rechtssicheren Rahmen für die Übermittlung von Daten in die USA geschaffen zu haben. Aktuell gelten die USA als sicheres Drittland gemäß DS-GVO. Es gibt allerdings bereits Ankündigungen aus dem Angemessenheitsbeschluss zum EU-US Data Privacy Framework gerichtlich prüfen zu lassen.

Wie sicher ist Microsoft 365?

Die Plattform genügt allen gängigen Sicherheitsstandards für Cloud Plattformen.

Wo kann ich mehr zum Datenschutz von Microsoft 365 erfahren?

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

Thema Datenschutz für junge Leute - <https://privacy.microsoft.com/de-de/young-people>

Nutzungsvereinbarung pädagogisches Netz und Microsoft 365
sowie datenschutzrechtliche Informationen gemäß Art. 13 DS-GVO:

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 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 Microsoft 365?

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

Achtung - diese Seiten verbleiben beim Benutzer, damit Du / Sie jederzeit nachsehen kannst / können, wie die Nutzungsvereinbarungen lauten, welche personenbezogenen Daten verarbeitet werden und wie man als Betroffener seine Rechte gegenüber der Schule als verantwortliche Stelle geltend machen kann.