

Datenschutzinformationen

Microsoft Office 365 - Datenschutzinformation

Datenschutzrechtliche Informationen nach Art. 13 DS-GVO

Zur Nutzung von Office 365 am Grabbe-Gymnasium oder von zu Hause ist die Verarbeitung von personenbezogenen Daten erforderlich. Darüber möchten wir Sie im Folgenden informieren.

Datenverarbeitende Stelle Christian-Dietrich-Grabbe-Gymnasium Detmold, Küster-Meyer-Platz 2, 32756 Detmold, Tel.: 05231 99260 sekretariat@grabbe.nrw.schule

Schulischer Datenschutzbeauftragter s. Ansprechpartner:innenliste auf der Homepage

Zwecke der Verarbeitung personenbezogener Daten

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

Rechtsgrundlage der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten bei Nutzung von Microsoft Office Office 365 erfolgt auf der Grundlage von DS-GVO Art. 6

Kategorien betroffener Personen

Schülerinnen und Schüler des Grabbe-Gymnasiums

Kategorien von personenbezogenen Daten

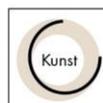
- Anmeldeinformationen, Rechte und Rollen, Zuteilung zu Gruppen, Geräte- und Nutzungsdaten, Nutzungsdaten von Inhalten, Interaktionen, Suchvorgänge und Befehle, Text-, Eingabe- und Freihanddaten, [Positionsdaten - vor allem bei BYOD und außerschulischer Nutzung relevant], Inhalte [1], Lizenzinformationen (Anzahl Installationen, bei Nutzung von Microsoft Office 365 Pro)

Kategorien von Empfängern

Intern:

- Schulische Administratoren (alle technischen Daten und Kommunikationsdaten, soweit für administrative Zwecke erforderlich)
- Schulleitung (Zugangsdaten, alle technischen Daten und Kommunikationsdaten im begründeten Verdachtsfall einer Straftat oder bei offensichtlichem Verstoß gegen die Nutzungsvereinbarung),

[1] Details siehe <https://privacy.microsoft.com/de-de/privacystatement#mainenterprise-developer-products-modules> (soweit auf Microsoft Office 365 Education zutreffend)



Extern:

- Microsoft Office (zur Bereitstellung der Dienste von Microsoft Office 365, auf Weisung der Schulleitung, OST vom [Datum des Vertragsabschlusses/ Verlinkung der OST])
- Dienstleister, Administratoren (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich, auf Weisung der Schulleitung)
- Ermittlungsbehörden (alle Daten betroffener Benutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- Betroffene (Auskunftsrecht nach Art. 15 DS-GVO)

Löschfristen

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

- Alle Daten im Zusammenhang mit dem Konto des Benutzers werden von Microsoft Office 30 Tage aufbewahrt. Eine Ausnahme bilden Daten mit gesetzlicher Aufbewahrungspflicht, die entsprechend lange 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.[2]

[2] Siehe Verwalten der Lizenzen und Inhalte von Absolventen in Microsoft 365 Education (11/2018)

Benutzer müssen ihre Daten vorher eigenständig sichern.

Recht auf Widerruf

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

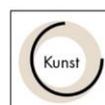
Weitere Betroffenenrechte

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

Microsoft 365 – Nutzungsvereinbarung

Für alle Tätigkeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhalten Sie Zugang zu unserer Arbeitsplattform Microsoft Office365.

Den Zugang zu Microsoft Office365 stellen wir Ihnen auch außerhalb des Unterrichts zur schulischen Nutzung Verfügung.



Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, der Arbeitsplattform Microsoft Office 365 sowie den eigenen personenbezogenen Daten und denen von anderen in der Schule lernenden und arbeitenden Personen voraus.

Die folgende Nutzungsvereinbarung informiert und steckt den Rahmen für eine verantwortungsvolle Nutzung ab.

Geltungsbereich

Die Nutzungsvereinbarung gilt für Personengruppen, nachfolgend "Benutzer" genannt, welche Microsoft Office 365 zur elektronischen Datenverarbeitung nutzen.

Laufzeit

Dem Benutzer werden innerhalb seiner Schulzeit/ Dienstzeit ein Benutzerkonto samt Microsoft Office 365 zur Verfügung gestellt. Beim Verlassen der Schule wird das Benutzerkonto deaktiviert und gelöscht sowie die Zuweisung der Microsoft Office 365 A3 aufgehoben.

Umfang

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

- Zugang zu Microsoft Office 365 (A3) mit
 - einer E-Mail-Adresse
 - Online Speicherplatz auf Microsoft OneDrive
 - Microsoft Online (Word, Excel, PowerPoint, OneNote, Teams, Sway, [...])
 - Nutzung von Microsoft Office als Desktop-Anwendung

Datenschutz und Datensicherheit

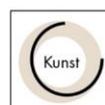
Microsoft verpflichtet sich, die personenbezogenen Daten von Benutzern in Microsoft Office 365 nicht zur Erstellung von Profilen zur Anzeige von Werbung oder Direkt Marketing zu nutzen. Ziel unserer Schule ist es, durch eine Minimierung von personenbezogenen Daten bei der Nutzung von Microsoft Office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

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

Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, der Arbeitsplattform Microsoft Office 365 sowie den eigenen personenbezogenen Daten und denen von anderen in der Schule lernenden und arbeitenden Personen voraus.

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

Verantwortungsvolles und sicheres Handeln bedeutet:



Passwörter

- müssen sicher sein und dürfen nicht erratbar sein. Sie müssen aus mindestens 8 Zeichen bestehen, worunter sich eine Zahl, ein Großbuchstabe und ein Sonderzeichen befinden müssen.

Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum persönlichen Microsoft Office 365 Konto geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben werden.
- Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist der Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist ein schulischer Administrator zu informieren.
- Sollte der Benutzer in Kenntnis fremder Zugangsdaten gelangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Der Benutzer ist jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.

Personenbezogene Daten

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

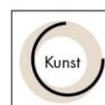
Urheberrecht

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

Unzulässige Inhalte und Handlungen

Benutzer sind verpflichtet, bei der Nutzung von Microsoft Office 365 geltendes Recht einzuhalten.

- Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über Microsoft Office 365 abzurufen, zu speichern oder zu verbreiten.



- Die geltenden Jugendschutzvorschriften sind zu beachten.
- Die Verbreitung und das Versenden von belästigenden, verleumderischen oder bedrohenden Inhalten sind unzulässig.
- Die E-Mail Funktion von Microsoft Office 365 darf nicht für die Versendung von Massennachrichten (Spam) und/oder anderen Formen unzulässiger Werbung genutzt werden.

Zu widerhandlungen

Im Falle von Verstößen gegen diese Nutzungsordnung behält sich die Schulleitung das Recht vor, den Zugang zu einzelnen oder allen Bereichen innerhalb von Microsoft Office 365 zu sperren. Davon unberührt behält sich die Schulleitung weitere dienstrechtliche Maßnahmen oder Ordnungsmaßnahmen vor.

Nutzungsbedingungen von Microsoft für Microsoft Office 365

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

Verhaltenskodex

Inhalte, Materialien oder Handlungen, die diese Bestimmungen verletzen, sind unzulässig. Mit Ihrer Zustimmung zu diesen Bestimmungen gehen Sie die Verpflichtung ein, sich an diese Regeln zu halten: 1. Nehmen Sie keine unrechtmäßigen Handlungen vor.

2. Unterlassen Sie Handlungen, durch die Kinder ausgenutzt werden, ihnen Schaden zugefügt oder angedroht wird.

3. Versenden Sie kein Spam. Bei Spam handelt es sich um unerwünschte bzw. unverlangte Massen-E-Mails, Beiträge, Kontaktanfragen, SMS (Textnachrichten) oder Sofortnachrichten.

4. Unterlassen Sie es, unangemessene Inhalte oder anderes Material (das z. B. Nacktdarstellungen, Brutalität, Pornografie, anstößige Sprache, Gewaltdarstellungen oder kriminelle Handlungen zum Inhalt hat) zu veröffentlichen oder über die Dienste zu teilen.

5. Unterlassen Sie Handlungen, die betrügerisch, falsch oder irreführend sind (z. B. unter Vorspiegelung falscher Tatsachen Geld fordern, sich als jemand anderes ausgeben, die Dienste manipulieren, um den Spielstand zu erhöhen oder Rankings, Bewertungen oder Kommentare zu beeinflussen).

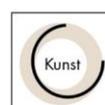
6. Unterlassen Sie es, wissentlich Beschränkungen des Zugriffs auf bzw. der Verfügbarkeit der Dienste zu umgehen.

7. Unterlassen Sie Handlungen, die Ihnen, dem Dienst oder anderen Schaden zufügen (z. B. das Übertragen von Viren, das Belästigen anderer, das Posten terroristischer Inhalte, Hassreden oder Aufrufe zur Gewalt gegen andere).

8. Verletzen Sie keine Rechte anderer (z. B. durch die nicht autorisierte Freigabe von urheberrechtlich geschützter Musik oder von anderem urheberrechtlich geschütztem Material, den Weiterverkauf oder sonstigen Vertrieb von Bing-Karten oder Fotos).

9. Unterlassen Sie Handlungen, die die Privatsphäre von anderen verletzen.

10. Helfen Sie niemandem bei einem Verstoß gegen diese Regeln



Nutzungsordnung für IServ

Christian-Dietrich-Grabbe-Gymnasium Küster-Meyer-Platz 2

32756 Detmold

Telefon: (05231) 9926-0

Telefax: (05231) 9926-16

1. Januar 2021

Präambel

Die Schule stellt ihren Schülerinnen, Schülern und Lehrkräften (im Folgenden: Nutzer) als Kommunikations- und Austauschplattform IServ zur Verfügung. IServ dient ausschließlich der schulischen Kommunikation und ermöglicht allen Nutzern, schulbezogene Daten zu speichern und auszutauschen. Alle Nutzer verpflichten sich, die Rechte anderer Personen zu achten.

Nutzungsmöglichkeiten

Die Schule entscheidet darüber, welche Module von IServ für den innerschulischen Gebrauch freigeschaltet werden. Welche Module freigeschaltet sind, teilt die Schule den Nutzern in allgemeiner Form mit.

Verhaltensregeln

Jeder Nutzer erhält ein Nutzerkonto. Das Nutzerkonto muss durch ein nicht zu erratendes Passwort von mindestens acht Zeichen Länge (Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen) gesichert werden. Es ist untersagt, das Passwort anderen Nutzern mitzuteilen.

Die im gemeinsamen Adressbuch eingegebenen Daten sind für alle Nutzer sichtbar. Es wird deshalb geraten, so wenig personenbezogene Daten wie möglich von sich preiszugeben.

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

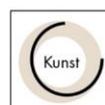
Die Nutzer verpflichten sich, die gesetzlichen Regelungen des Straf- und Jugendschutzgesetzes sowie das Urhebergesetz zu beachten. Wer Dateien auf IServ hoch lädt, über IServ versendet oder nutzt, tut dies in eigener Verantwortung. Die Schule übernimmt keine Verantwortung für die Inhalte und die Art gespeicherter Daten.

Die Sicherung in IServ gespeicherter Daten gegen Verlust obliegt der Verantwortung der Nutzer.

Das Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte auf dem Schulserver ist ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten.

Weil umfangreiche Up- und Downloads die Arbeitsgeschwindigkeit des Servers beeinträchtigen, sind diese nicht erlaubt. Ausnahmen sind vorab mit den Administratoren abzusprechen.

Die Installation oder Nutzung fremder Software durch die Nutzer ist nicht zulässig, sie darf nur von den Administratoren durchgeführt werden.



Das IServ-System erstellt Log-Dateien (Protokolle), die in begründeten Fällen (z. B. Bei Rechtsverstößen oder Täuschungsversuchen) von den von der Schulleitung bestimmten Personen ausgewertet werden können.

Kommunikation E-Mail

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

Der E-Mail-Account wird nur für den Austausch von Informationen im schulischen Zusammenhang bereitgestellt.

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

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

Messenger

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

Forum

Soweit die Schule eine Forum-Funktion zur Verfügung stellt, gelten dieselben Vorgaben wie bei der E-Mail-Nutzung. Darüber hinaus sind die Moderatoren der Foren berechtigt, unangemessene Beiträge zu löschen.

Die Nutzer verpflichten sich, in Foren, Chats und von IServ aus versendeten E-Mails die Rechte anderer zu achten. Massen-E-Mails, Joke-E-Mails o. ä. sind nicht gestattet.

Die schulische E-Mail-Adresse darf nicht für private Zwecke zur Anmeldung bei Internetangeboten jeder Art verwendet werden. Das gilt insbesondere für alle sozialen Netzwerke wie z. B. Facebook oder Google+.

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

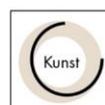
Hausaufgaben

Hausaufgaben können über IServ gestellt werden, müssen aber im Unterricht angekündigt werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum.

Administratoren

Die Administratoren haben weitergehende Rechte, verwenden diese aber grundsätzlich nicht dazu, sich Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen.

Sollte ein Nutzer sein Passwort vergessen haben, ist er verpflichtet, das durch einen Administrator neu vergebene Passwort beim nächsten Einloggen sofort zu ändern. Nur der Nutzer selbst darf ein neues Passwort für sich persönlich bei einem Administrator beantragen.



Moderatoren

Für die Gruppenforen können Moderatoren eingesetzt werden, die Forumsbeiträge auch löschen können. Moderatoren dürfen nur in dem ihnen anvertrauten Forum moderieren.

Verstöße

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

Schulung

Eine Schulung erfolgt für entweder lokal oder multimedial zu festgelegten Zeiten im jeweiligen Schuljahr.

Nutzungsordnung für WebUntis

Christian-Dietrich-Grabbe-Gymnasium Küster-Meyer-Platz 2, 32756 Detmold

Am Grabbe-Gymnasium nutzen Schüler der Oberstufe, Eltern und Lehrkräfte WebUntis als digitalen Stunden- und Vertretungsplan. Damit das möglich ist, werden auch personenbezogene Daten der Benutzer verarbeitet, von der Schule und von WebUntis GmbH. Hiermit möchten wir Ihnen alle wichtigen Informationen dazu geben.

Für wen gelten diese Datenschutzhinweise?

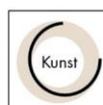
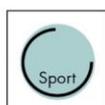
- Diese Informationen zur Datenverarbeitung im Zusammenhang mit der Nutzung von WebUntis gelten für alle schulischen Nutzer von WebUntis, Schüler:innen der Oberstufe, Erziehungsberechtigte und Lehrkräfte.

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

- Christian-Dietrich-Grabbe-Gymnasium, Detmold , Kontaktdaten auf der Homepage

Welche Daten werden verarbeitet und woher kommen sie?

- Bei der Nutzung von WebUntis über Browser oder App geht es um folgende personenbezogene Daten:
 - Anmeldeinformationen (Benutzer, Passwort) werden für jeden Nutzer (Schüler:innen der Oberstufe, Lehrkräfte) von der Schule erstellt. Erziehungsberechtigte erstellen ihr Passwort selbst, hier ist nur die der Schule bekanntgemachte Email-Adresse mit dem zugehörigen Kind verknüpft.
 - Die Zuordnung zu Gruppen und die damit verbundenen Rollen und Rechte, die Spracheinstellung und der Kontostatus erfolgen anhand von Informationen aus der Schulverwaltung.
 - Weitere Daten entstehen bei der Nutzung von WebUntis zum Abrufen des digitalen Stunden- und Vertretungsplans. Das sind:
 - Server-Logdaten (z.B. Browsertyp und -version, Betriebssystem, IP Nummer)
 - Von WebUntis erhobene Nutzungsdaten (IP Adresse, letzter Login)
 - Vom Benutzer eingestellte Profildaten (z.B. Adresse, Telefonnummer)
 - Bei Lehrkräften, vom Benutzer erzeugte Inhaltsdaten (z.B. Notizen für Schüler:innen/ für Lehrkräfte, gebuchte Ressourcen, verschickte Nachrichten)
 - Vom Nutzer angemeldete Geräte zum Zugriff auf WebUntis und Aktivierung von Zwei-Faktor-Authentifizierung



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

- Bereitstellung eines Zugangs zu WebUntis
- Nutzung von WebUntis durch angemeldete Nutzer
- Verwaltung von Rechten und Rollen der Benutzer entsprechend der Funktion (Schüler:in / Lehrkraft / Erziehungsberechtigte) und der Zugehörigkeit zu Stufen
- Technische Bereitstellung von für die Verwaltung und Nutzung der WebUntis erforderlichen Diensten
- Sicherheit und Funktionalität dieser Dienste

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 und § 3 Abs. 1 DSG NRW.

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

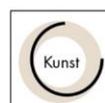
- Die Nutzung von WebUntis ist nur möglich, wenn man dafür von WebUntis GmbH bereitgestellte Dienste nutzt. Dieses sind Dienste zur Verwaltung von Nutzern und Inhalten. Auftragsverarbeiter - nach Weisung durch die Schulleitung
 - Von der Schule / vom Schulträger beauftragter Dienstleister WebUntis GmbH
 - Innerhalb der Schule wird der Zugriff auf die Daten im Zusammenhang mit der Nutzung von WebUntis durch das Rechte- und Rollenkonzept geregelt.
 - Schulleitungsmitglieder - alle Daten, ohne administrative Rechte
 - Schulische Administratoren - alle Daten aller Personen (auf Weisung der Schulleitung)
 - Lehrkräfte - eigene Daten; [alle/eigene] Stunden-/ Vertretungspläne einsehen
 - Schüler:innen der Oberstufe - eigene Daten; eigene Stufen- und Vertretungspläne
 - Personen von außerhalb der Schule erhalten nur Zugriff auf Daten, wenn ein Gesetz es ihnen gestattet
 - Eltern über das Konto ihrer Kinder: eigene Daten Schüler:in; Stunden- und Vertretungspläne des Kindes
 - Ermittlungsbehörden im Fall einer Straftat

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

- Nein. Die Server unseres Anbieters stehen in Österreich, kein Drittland nach DS-GVO

Findet eine automatisierte Entscheidungsfindung statt?

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



Wie lange werden meine Daten gespeichert?

- Die Benutzerdaten von Schüler:innen und Lehrkräften im Zusammenhang mit dem Zugang zu WebUntis über Browser und App (Kontodaten) werden solange gespeichert wie diese
 - WebUntis nutzen
 - An der Schule Schüler:in oder Lehrkraft sind
 - Nach Beendigung der Nutzung des Zugangs zu WebUntis, Verlassen Schule bzw. Ende des Dienstes an Schule werden die Kontodaten des Benutzers innerhalb von sechs Wochen endgültig aus WebUntis gelöscht. WebUntis GmbH löscht sämtliche Daten danach von allen Servern und Sicherheitskopien in einem Zeitraum von 6 Monaten.
 - Durch Lehrkräfte eingetragene Informationen in Stunden- und Vertretungsplänen werden entsprechend VO-DV I §9 bzw. VO-DV II §9 für 5 Jahre aufbewahrt.
 - Daten im Zusammenhang mit der Erstellung von Verwaltung von Benutzerkonten für die Nutzung der WebUntis, die in der Schulverwaltung vorliegen, werden entsprechend VO-DV I §9 bzw. VO-DV II §9 für 5 Jahre aufbewahrt.
 - Benutzer haben jederzeit die Möglichkeit, von ihnen eingestellte Kontaktdaten und Freigaben eigenständig zu löschen.

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.

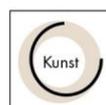
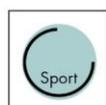
Recht zur Beschwerde bei der Aufsichtsbehörde

- Zudem steht Ihnen ein Beschwerderecht bei der Datenschutzaufsichtsbehörde, der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen zu.

Wo finde ich weitere Informationen zum Thema Datenschutz und WebUntis?

- Weitere Informationen unter <https://www.untis.at/warum-untis/ueber-das-produkt/datenschutz-und-sicherheit>

Hinweis: Die Verarbeitung von personenbezogenen Daten, die bei der Nutzung der WebUntis Android und iOS App auf dem Endgerät des Nutzers anfallen, liegen nicht in der Verantwortung der Schule. In dieser Datenschutzerklärung geht es lediglich um die Daten, welche beim Zugriff über diese Apps durch den Nutzer auf das WebUntis der Schule anfallen.



Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I)

Vom 14. Juni 2007 (Fn [1](#))

Aufgrund des § 122 Abs. 4 des Schulgesetzes NRW (SchulG) vom 15. Februar 2005 ([GV. NRW. S. 102](#)), zuletzt geändert durch Artikel 1 des Gesetzes vom 27. Juni 2006 ([GV. NRW. S. 278](#)), wird mit Zustimmung des Ausschusses für Schule und Weiterbildung des Landtags verordnet:

§ 1 (Fn [2](#)) Zulässigkeit der Datenverarbeitung, Datensicherheit

§ 1 (Fn [2](#))

Zulässigkeit der Datenverarbeitung, Datensicherheit

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

1. der Schülerinnen und Schüler,
2. der Eltern gemäß § 123 SchulG,
3. der Verpflichteten gemäß § 41 SchulG

in Dateien und/oder Akten zu verarbeiten, soweit diese Verordnung oder andere Rechtsvorschriften dies zulassen.

(2) Die zur Verarbeitung zugelassenen Daten sind in den Anlagen genannt. Die nicht für die automatisierte Datenverarbeitung zugelassenen Daten sind in den Anlagen besonders gekennzeichnet. Sofern die Erfüllung der übertragenen Aufgaben die Verarbeitung von in den Anlagen nicht genannten Daten im Einzelfall erforderlich macht, gelten die allgemeinen datenschutzrechtlichen Vorschriften. Die Zulässigkeit der Verarbeitung erstreckt sich auch auf in der Anlage nicht genannte Daten, soweit sie aus den in den Anlagen genannten Daten gebildet oder abgeleitet werden und zur Erfüllung der übertragenen Aufgaben erforderlich sind. Die Verarbeitung umfasst auch die Auswertungen von Daten, die zur Erfüllung der übertragenen Aufgaben erforderlich sind.

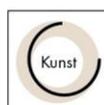
(3) Für die Schule stellt die Schulleiterin oder der Schulleiter, für die Schulaufsichtsbehörde die Leiterin oder der Leiter der Behörde durch technische oder organisatorische Maßnahmen sicher, dass der Schutz der verarbeiteten Daten gemäß § 10 DSGVO gewährleistet ist und die Löschungsbestimmungen eingehalten werden. Die Zuständigkeit der gemäß § 1 Abs. 6 VO-DV II bestellten behördlichen Datenschutzbeauftragten (§ 32 a DSGVO) besteht auch für die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften in Bezug auf die Daten der Schülerinnen, Schüler und Eltern.

§ 2 (Fn [2](#)) Verfahren der automatisierten Datenverarbeitung

§ 2 (Fn [2](#))

Verfahren der automatisierten Datenverarbeitung

(1) Die automatisierte Verarbeitung der personenbezogenen Daten ist zulässig auf ADV-Arbeitsplätzen und in Netzwerken, die für Verwaltungszwecke eingerichtet sind, auf sonstigen schulischen ADV-Anlagen und in sonstigen Netzwerken, wenn jeweils über die Konfiguration die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz gemäß § 10 des Datenschutzgesetzes Nordrhein-



Westfalen gewährleistet sind. Insbesondere ist sicherzustellen, dass Berechtigte nur Zugang zu personenbezogenen Daten erhalten, die für die jeweilige Aufgabenerfüllung erforderlich sind.

(2) Die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern in privaten ADV-Anlagen von Lehrerinnen und Lehrern für dienstliche Zwecke bedarf der schriftlichen, ein Verzeichnisses gemäß § 8 DSGVO NRW enthaltenden Genehmigung durch die Schulleiterin oder den Schulleiter. Die Genehmigung darf nur erteilt werden, wenn die Verarbeitung der Daten nach Art und Umfang für die Erfüllung der schulischen Aufgaben erforderlich ist und ein angemessener technischer Zugangsschutz nachgewiesen wird. Die für die Verarbeitung zugelassenen Daten ergeben sich aus der Anlage 3. Für die nach Satz 1 genehmigte Verarbeitung personenbezogener Daten in privaten ADV-Anlagen ist die Schule öffentliche Stelle im Sinne des § 2 Abs. 1 und 2 Satz 3 DSGVO NRW. Die Lehrerinnen und Lehrer sind verpflichtet, der Schulleiterin oder dem Schulleiter alle Auskünfte zu erteilen, die für die datenschutzrechtliche Verantwortung erforderlich sind.

(3) Die Schulen und Schulaufsichtsbehörden sind berechtigt, unter Beachtung der Voraussetzung des § 11 DSGVO NRW die Datensicherheit gewährleistende und zuverlässige Institutionen mit der Verarbeitung ihrer Daten zu beauftragen. Die Datenverarbeitung im Auftrag ist nur zulässig nach Weisung der Schule oder der Schulaufsichtsbehörden und ausschließlich für deren Zwecke.

§ 3 (Fn 2) Datenerhebung, Berichtigung, Auskunft, Einsicht in Akten

§ 3 (Fn 2)

Datenerhebung, Berichtigung, Auskunft, Einsicht in Akten

(1) Die in § 1 Abs. 1 genannten Personen sind bei der Erhebung personenbezogener Daten zur Auskunft verpflichtet, soweit es sich um Daten handelt, die in den Anlagen aufgeführt sind.

(2) Nicht in den Anlagen aufgeführte Daten dürfen nur erhoben werden, wenn die oder der Betroffene eingewilligt hat. Die Einwilligung ist schriftlich gegenüber der Schulleitung zu erklären. Sofern dies wegen besonderer Umstände angemessen ist, kann die Einwilligung ausnahmsweise in elektronischer Form erfolgen. Dabei sind die Grundsätze des § 13 Absatz 2 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBl. I S. 1766) geändert worden ist, zu erfüllen. Auch mit Einwilligung dürfen unzumutbare, nicht zweckdienliche oder sachfremde Angaben nicht erhoben werden.

(3) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(4) Die in § 1 Abs. 1 genannten Personen sind mit den Einschränkungen des § 120 Abs. 7 SchulG berechtigt, Einsicht in die sie betreffenden Unterlagen zu nehmen und Auskunft über die sie betreffenden Daten und die Stellen zu erhalten, an die Daten übermittelt worden sind.

§ 4 (Fn 2) Datenbestand in der Schule

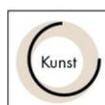
§ 4 (Fn 2)

Datenbestand in der Schule

(1) Bei der Aufnahme einer Schülerin oder eines Schülers legt die Schule ein Schülerstammblatt an.

(2) In das Schülerstammblatt sind aufzunehmen:

1. die Personaldaten der in § 1 Abs. 1 Nr. 1 - 3 genannten Personen (Individualdaten) gemäß Abschnitt A Nr. I der Anlage 1,



2. die Information zur schulischen Laufbahn der Schülerin oder des Schülers (Organisations- bzw. Schullaufbahndaten) gemäß Abschnitt A Nr. II der Anlage 1,
3. die Angaben über den individuellen Leistungsstand der Schülerin oder des Schülers (Leistungsdaten) gemäß Abschnitt B der Anlage 1,
4. die für die einzelnen Schulformen oder Schulstufen benötigten zusätzlichen Informationen (schulform- oder schulstufenspezifische Zusatzdaten) gemäß Abschnitt C der Anlage 1.

(3) Für die Anlage des Schülerstammblasses ist die Schulleiterin oder der Schulleiter verantwortlich. Das Schülerstammblass wird in einfacher Ausfertigung geführt, bei automatisierter Verarbeitung zusätzlich in Papieraufbereitung.

(4) Die Klassenlehrerin oder der Klassenlehrer, im Kurssystem der gymnasialen Oberstufe die Jahrgangsstufenleitung (die Beratungslehrerin oder der Beratungslehrer), sorgt für die Aktualität des Schülerstammblasses und erledigt die damit zusammenhängenden Aufgaben. Eintragungsberechtigt sind daneben die Mitglieder der Schulleitung und in besonderen Fällen weitere von der Schulleiterin oder dem Schulleiter benannte Personen.

(5) Neben dem Schülerstammblass führt die Schule in Papieraufbereitung die in der Anlage 2 aufgeführten Dateien und Akten (sonstiger Datenbestand); eine Verarbeitung in ADV-Anlagen ist mit den Einschränkungen des § 1 Abs. 2 zulässig.

(6) Das Schülerstammblass und der sonstige Datenbestand können von allen Lehrerinnen und Lehrern der Schülerin oder des Schülers, der Beratungslehrerin oder dem Beratungslehrer, Lehramtsanwärterinnen und Lehramtsanwärttern sowie Studienreferendarinnen und Studienreferendaren eingesehen werden, soweit dies zur Erfüllung der Aufgaben dieser Personen erforderlich ist. Die Genehmigung erteilt im Einzelfall oder generell die Schulleiterin oder der Schulleiter. Das Recht auf Einsichtnahme durch Schulaufsichtsbeamtinnen und Schulaufsichtsbeamte im Rahmen ihrer Aufgaben bleibt unberührt.

§ 5 (Fn 2) Allgemeine Bestimmungen für die Übermittlung von Daten

§ 5 (Fn 2)

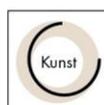
Allgemeine Bestimmungen für die Übermittlung von Daten

(1) Die Übermittlung von personenbezogenen Daten an öffentliche Stellen oder an Stellen außerhalb des öffentlichen Bereichs richtet sich nach § 120 Abs. 5 SchulG.

(2) Die Datenübermittlung kann schriftlich, mündlich, automatisiert oder auf Datenträgern erfolgen. Datenträger, die versandt werden, dürfen personenbezogene Daten nur enthalten, soweit diese für die Empfängerin oder den Empfänger bestimmt sind. Eine automatisierte Datenübermittlung kann auch über eine gemeinsam genutzte informationstechnische Basis-Infrastruktur erfolgen, sofern die technischen und organisatorischen Sicherheitsanforderungen des § 10 des Datenschutzgesetzes Nordrhein-Westfalen erfüllt werden. Eine Datenübermittlung auf Datenträgern bedarf einer Verschlüsselung nach dem aktuellen Stand der Technik. Automatisierte Verfahren, die die Übermittlung personenbezogener Daten durch Abruf ermöglichen, sind unzulässig.

(3) Das für die Schule zuständige Ministerium kann zum Zwecke der einheitlichen Erfüllung der datenschutzrechtlichen Bestimmungen für die

1. zur Übermittlung von Daten einzusetzende Hard- und Software,



2. zur Übermittlung von Daten einzusetzenden Verfahren,

3. Maßnahmen und Verfahren zur Einhaltung der datenschutzrechtlichen Bestimmungen auf dem Übermittlungswege

Rahmenbedingungen schaffen oder im Einvernehmen mit den Schulträgern den Einsatz bestimmter Hardware, Software, Maßnahmen oder Verfahren vorschreiben.

§ 6 Datenübermittlung bei einem Schulwechsel

§ 6 Datenübermittlung bei einem Schulwechsel

(1) Bei einem Schulwechsel übermittelt die abgebende Schule der aufnehmenden Schule personenbezogene Daten aus dem Schülerstammblatt und dem sonstigen Datenbestand, soweit die Daten für die weitere Schulausbildung der Schülerin oder des Schülers erforderlich sind. Entsprechendes gilt bei der Kooperation von Schulen. Die Unterlagen selbst verbleiben bei der abgebenden Schule.

(2) Folgende Daten werden übermittelt:

1. Individualdaten der in § 1 Abs. 1 Nr. 1 - 3 genannten Personen (Anlage 1, Abschnitt A, Nr. I),
2. Daten über den sonderpädagogischen Förderbedarf und die sonderpädagogische Förderung (Anlage 1, Abschnitt C, Nr. IV) sowie über gesundheitliche Beeinträchtigungen und/oder körperliche Behinderungen (Anlage 1, Abschnitt A, Nr. II, Ziffer 13), soweit für Schülerinnen und Schüler eine besondere schulische Betreuung in Betracht kommt,
3. Daten über Schulbesuchszeiträume, über die bisher besuchten Schulen und Klassenwiederholungen (mit Gründen),
4. Daten über erreichte Schul- oder Ausbildungsabschlüsse sowie Einzelinformationen, die für die neu begonnene Schullaufbahn unerlässlich sind (z.B. bisheriger Fremdsprachen- und naturwissenschaftlicher Unterricht, die Kurswahl und Leistungsergebnisse ab Jahrgangsstufe 11 der gymnasialen Oberstufe),
5. eine Zweitschrift des letzten Zeugnisses oder bei der Anmeldung für die weiterführende Schule auch des Halbjahreszeugnisses.

Die Eltern sind von der abgebenden Schule über die Übermittlung der Daten gemäß Nummer 2 zu unterrichten.

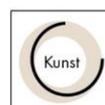
(3) Die Übermittlung der Daten nach Absatz 2 kann auch schon bei der Anmeldung erfolgen.

§ 7 Datenübermittlung zum Zwecke der Schulpflichtüberwachung

§ 7 Datenübermittlung zum Zwecke der Schulpflichtüberwachung

(1) Zur Überwachung der Schulpflicht übermittelt die abgebende Schule der aufnehmenden Schule personenbezogene Daten schulpflichtiger Schülerinnen und Schüler sowie in § 1 Abs. 1 Nr. 2 und 3 genannter Personen nach Maßgabe der Absätze 2, 3 und 5. Die aufnehmende Schule übermittelt der abgebenden Schule die Aufnahmeentscheidung. Die Überwachung der Schulpflicht obliegt solange der abgebenden Schule, bis ihr die Aufnahme durch die aufnehmende Schule übermittelt wurde.

(2) Zur Überwachung der Schulpflicht werden der aufnehmenden Schule folgende Daten der Betroffenen übermittelt:



1. Name, Vorname, Geburtsname,
2. Geburtsdatum, -ort und -land,
3. Geschlecht,
4. Staatsangehörigkeit,
5. Erreichbarkeit,
6. Name und Erreichbarkeit der in § 1 Abs. 1 Nr. 2 und 3 genannten Personen,
7. Schülernummer/Nummer des Gesamtschülerverzeichnisses,
8. Datum der ersten Einschulung,
9. Klasse/Jahrgang,
10. Angaben zu Schulbesuch/Schulversäumnis.

(3) Zur Überwachung der Schulpflicht in der Sekundarstufe II werden der aufnehmenden Schule neben den Daten des Absatzes 2 folgende Daten der Betroffenen übermittelt:

1. Angaben zur bisherigen Schulbildung und zur zuletzt besuchten Schule,
2. Angaben zur angestrebten Ausbildung, insbesondere Angaben zur Berufsausbildung, zum Praktikanten- oder Arbeitsverhältnis.

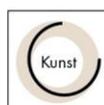
(4) Zur Überwachung der Schulpflicht in der Sekundarstufe II werden dem Ausbildungsbetrieb folgende Daten der Betroffenen übermittelt:

1. Name, Vorname, Geburtsname,
2. Geburtsdatum,
3. Geschlecht,
4. Erreichbarkeit,
5. Angaben zu unentschuldigtem Schulversäumnissen.

(5) Soweit erforderlich werden im Rahmen der Überwachung der Pflicht zum Besuch des Berufskollegs oder einer anderen Schule der Sekundarstufe II in den Fällen des Abgangs von der Schule und des Schulwechsels folgende Daten von der abgehenden Schule auch dem Schulträger zur Koordinierung des Übergangs in das Berufskolleg, in ein Berufsausbildungsverhältnis oder in eine andere Schule der Sekundarstufe II übermittelt:

1. Name, Vorname, Geburtsname,
2. Geburtsdatum, -ort und -land,
3. Geschlecht,
4. Erreichbarkeit,
5. Name und Erreichbarkeit der in § 1 Abs. 1 Nr. 2 und 3 genannten Personen.

§ 8 Datenübermittlung zum Zwecke der Schulgesundheitspflege



§ 8

Datenübermittlung zum Zwecke der Schulgesundheitspflege

(1) Zur Durchführung von Maßnahmen der Schulgesundheitspflege übermittelt die Schule der unteren Gesundheitsbehörde personenbezogene Daten von Schülerinnen und Schülern sowie den Eltern.

(2) Folgende Daten der Betroffenen werden übermittelt:

1. Name, Vorname,
2. Geburtsdatum, -ort und -land,
3. Geschlecht,
4. Erreichbarkeit,
5. Name, Vorname und Erreichbarkeit der Eltern.

§ 9 Aufbewahrung, Aussonderung, Löschung und Vernichtung der Dateien und Akten

§ 9

Aufbewahrung, Aussonderung, Löschung und Vernichtung der Dateien und Akten

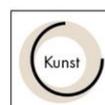
(1) Für personenbezogene Daten, die nach dieser Verordnung in Dateien gespeichert oder in Akten aufbewahrt werden, gelten folgende Fristen:

- | | |
|--|----------|
| 1. Zeitschriften von Abgangs- und Abschlusszeugnissen | 50 Jahre |
| 2. Schülerstammlätter | 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. |

Die Aufbewahrungsfristen beginnen mit Ablauf des Kalenderjahres, in dem die Akten oder Dateien abgeschlossen worden sind, jedoch nicht vor Ablauf des Kalenderjahres, in dem die Schulpflicht endet, sofern nichts anderes bestimmt ist.

(2) Sind die Daten nach Absatz 1 in öffentlichen ADV-Anlagen oder auf Datenträgern gespeichert, gelten die Aufbewahrungsfristen entsprechend. Für in privaten ADV-Anlagen gespeicherte Daten (§ 2 Abs. 2) beträgt die Aufbewahrungsfrist ein Jahr. Sie beginnt abweichend von Absatz 1 mit Ablauf des Kalenderjahres, in dem die Schülerin oder der Schüler von der Lehrerin oder dem Lehrer nicht mehr unterrichtet wird.

(3) Akten und Dateien, deren Aufbewahrungsfristen abgelaufen sind, sind mit Ausnahme der Dateien nach § 2 Abs. 2 dem zuständigen Archiv zur Übernahme anzubieten. Akten und Dateien, die nicht durch ein Archiv übernommen werden, sind zu vernichten oder zu löschen.



(4) Zur Führung der Schulchronik (Daten zur Schulgeschichte) dürfen Schulen die folgenden personenbezogenen Daten von Schülerinnen und Schülern zeitlich unbefristet verwenden:

1. Name, Geburtsname, Vorname, Geschlecht,
2. Geburtsdatum, Geburtsort, Geburtsland,
3. Anschrift,
4. Daten über die Dauer des Besuchs der Schule.

§ 10 Ordnungswidrigkeiten

§ 10 Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig als nach § 3 Abs. 1 zur Auskunft Verpflichteter

1. keine,
2. unrichtige oder
3. unvollständige

Auskunft erteilt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist die Bezirksregierung.

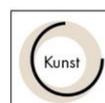
§ 11 In-Kraft-Treten, Berichtspflicht

§ 11 In-Kraft-Treten, Berichtspflicht

(1) Diese Verordnung tritt am Tage nach der Verkündung in Kraft. Gleichzeitig tritt die Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Erziehungsberechtigten (VO-DV I) vom 24. März 1995 (GV. NRW. S. 356), zuletzt geändert durch Artikel 9 des Gesetzes vom 8. Juli 2003 ([GV. NRW. S. 413](#)), außer Kraft.

(2) Die Auswirkungen dieser Verordnung werden nach einem Erfahrungszeitraum von fünf Jahren durch die Landesregierung überprüft. Die Landesbeauftragte für Datenschutz und Informationsfreiheit ist an dieser Überprüfung zu beteiligen. Die Landesregierung unterrichtet den Landtagsausschuss für Schule und Weiterbildung bis zum 31. Dezember 2011 über das Ergebnis der Prüfung.

Die Ministerin
für Schule und Weiterbildung
des Landes Nordrhein-Westfalen



Informationen gemäß Artikel 13 Absatz 1 und 2 sowie Artikel 14 Absatz 1 und 2 DSGVO aufgrund der Erhebung von personenbezogenen Daten

Im Zusammenhang mit der Erfüllung des schulischen Bildungs- und Erziehungsauftrags des **Christian-Dietrich-Grabbe-Gymnasiums** werden Ihre personenbezogenen Daten als **Schülerin, Schüler oder Elternteil** erhoben.

Bitte beachten Sie hierzu nachstehende Datenschutzhinweise:

1. Angaben zum Verantwortlichen

Verantwortlich für die Datenerhebung ist: **Anja Vothknecht**

Bezeichnung: **stellv. Schulleiterin (StD')**
Straße: **Küster-Meyer-Platz 2**
Postleitzahl: **32756**
Ort: **Detmold**
Telefon: **05231-9926-0**
E-Mail-Adresse: **schulleitung@grabbe.nrw.schule**
Internet-Adresse: **www.grabbe-gymnasium.de**

2. Angaben zum Vertreter der Verantwortlichen

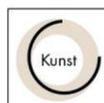
Die oben genannte Verantwortliche vertritt: **Dr. Claus Hilbing**

Bezeichnung: **komm. stellv. Schulleiter (StD')**
Straße: **Küster-Meyer-Platz 2**
Postleitzahl: **32756**
Ort: **Detmold**
Telefon: **05231-9926-0**
E-Mail-Adresse: **schulleitung@grabbe.nrw.schule**
Internet-Adresse: **www.grabbe-gymnasium.de**

3. Angaben zum Datenschutzbeauftragten

Die Kontaktadressen des Datenschutzbeauftragten lauten: **Dirk Meermann**

Bezeichnung: **Behördlicher Datenschutzbeauftragter
des Schulamtes des Kreises Lippe**
Straße: **Felix-Fechenbach-Straße 5**
Postleitzahl: **32756**
Ort: **Detmold**
Telefon: **05231-623550**
E-Mail-Adresse: **d.meermann@kreis-lippe.de**



4. Angaben zu der Aufsichtsbehörde

Zuständige Aufsichtsbehörde für den Datenschutz ist die
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen:

Straße: Kavalleriestr. 2-4
Postleitzahl: 40213 Düsseldorf
Telefon: 0211/38424-0
Telefax: 0211/38424-10
Email: poststelle@ldi.nrw.de
Internet: www.ldi.nrw.de

5. Kategorien der Daten, Zweck/e und Rechtsgrundlage/n der Verarbeitung

Personenbezogenen Daten von Schülerinnen, Schülern und Eltern werden zur Erfüllung der durch Rechtsvorschriften übertragenen Aufgaben erhoben.

Rechtsgrundlagen für die Verarbeitung Ihrer Daten sind:

Art. 6 Abs. 1 S. 1 Buchstabe e, Abs. 3, Art. 9 Abs. 2 Buchstabe g) EU-Datenschutzgrundverordnung (DSGVO) in Verbindung mit §§ 120-122 Schulgesetz (SchulG) sowie insbesondere die Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO DV I, einsehbar unter www.recht.nrw.de).

Dieser Verordnung können Sie insbesondere konkrete Daten entnehmen, die zur Verarbeitung zugelassen sind.

6. Evtl. Empfänger der personenbezogenen Daten (einschließlich des Zwecks der „Übermittlung“, der unter 5. bereits dargestellt ist)

Ihre personenbezogenen Daten können teilweise ggf. weitergegeben werden an eine aufnehmende Schule bei einem Schulwechsel: § 6 VO DV I

eine aufnehmende Schule oder den Schulträger bei einem Schulwechsel/Abgang von der Schule: § 7 VO DV I

die untere Gesundheitsbehörde zum Zwecke der Schulgesundheitspflege:
§ 8 VO DV I

Schulaufsichtsbehörden, den Schulträger und weitere Empfänger, soweit dies zur Erfüllung der dortigen per Rechtsvorschrift übertragenen Aufgaben im Einzelfall erforderlich ist: § 120 Abs. 5 SchulG

7. Absicht Übermittlung an Drittland oder eine internationale Organisation

- entfällt -

8. Dauer der Speicherung bzw. Kriterien für die Festlegung dieser Dauer

Ihre Daten werden nach Maßgabe der Aufbewahrungsfristen des § 9 VO DV I aufbewahrt und gelöscht.

9. Rechte der Betroffenen

Bei Erhebung personenbezogener Daten stehen Ihnen folgende Rechte zu:

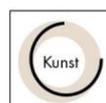
Sie haben nach Maßgabe der Artikel 15, 16, 17 und 18 EU-DSGVO gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

Recht auf Auskunft,

Recht auf Berichtigung oder Löschung,

Recht auf Einschränkung der Verarbeitung,

10. Widerrufsrecht bei Einwilligung



Sollten für einzelne Verarbeitungsvorgänge Ihrer Daten Einwilligungserklärungen erforderlich sein und deshalb gesondert eingeholt werden, können Sie Ihre Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird dadurch nicht berührt.

11. Beschwerderecht bei der Aufsichtsbehörde

Sie haben das Recht, bei der Landesbeauftragten für Datenschutz und Informationsfreiheit Beschwerde einzulegen, falls Sie der Auffassung sind, dass eine Verarbeitung Ihrer personenbezogener Daten gegen Datenschutzrecht verstößt. Die Kontaktdaten finden Sie unter Punkt 4. dieses Bogens.

12. Pflicht zur Bereitstellung der personenbezogenen Daten

Wenn Ihre personenbezogenen Daten unmittelbar bei Ihnen erhoben werden, sind Sie gemäß § 120 Abs. 2 Satz 1 SchulG zur Bereitstellung verpflichtet, soweit diese Daten zur Erfüllung der durch Rechtsvorschrift übertragenen Aufgaben der Schulen und Schulaufsichtsbehörden erforderlich sind.

13. Quelle der Daten

Wenn Daten nicht unmittelbar bei Ihnen erhoben wurden, können Sie stammen von einer abgebenden Schule bei einem Schulwechsel: §§ 6,7 VO DV I von einer Schulaufsichtsbehörde, dem Schulträger oder andere Behörden, soweit dies zur Erfüllung der dortigen per Rechtsvorschrift übertragenen Aufgaben im Einzelfall erforderlich ist: § 120 Abs. 5 SchulG

