

Informationsblatt zum Datenschutz, zur Nutzung der schulischen, digitalen Lernplattformen (MNS+, Nextcloud, bbb, Office 365), zur WLAN-Nutzung und zum Mobile Device Management (MDM) am Max-Slevogt-Gymnasium

Mit den folgenden Informationen möchten wir Ihnen (und Ihrem Kind) einen Überblick über die Verarbeitung Ihrer Daten am Max-Slevogt-Gymnasium und die Verhaltensweisen bei der Nutzung der digitalen Infrastruktur geben:

1. Wer ist für die Datenverarbeitung verantwortlich und an wen kann ich mich wenden?

Verantwortlich ist das Max-Slevogt-Gymnasium, Hindenburgstraße 2, 76829 Landau.

Bei Fragen, Beschwerden oder Anregungen steht Ihnen die Schulleitung in Kooperation mit dem schulischen Datenschutzbeauftragten, Herrn Dr. Wagner, zur Verfügung. Diesen erreichen Sie unter wag@msg.bildung-rp.de.

2. Zu welchem Zweck werden Ihre Daten und die Ihres Kindes verarbeitet?

Die Daten werden zur Erfüllung unseres Bildungs- und Erziehungsauftrages nach § 67 Schulgesetz und den dazugehörigen Schulordnungen verarbeitet. In Bezug auf die Eltern handelt es sich in erster Linie um Kontaktdaten; in Bezug auf die Schülerinnen und Schüler um Schulverwaltungsdaten und für die pädagogische Arbeit notwendige Daten. Hierzu gehören auch Schulnoten. Die entsprechenden Daten werden über das landeseigene Verwaltungsprogramm edoo.sys RLP verarbeitet.

Im cloudbasierten und DSGVO-konformen Vertretungsplanmodul WebUntis werden Name, Vorname, Geburtsdatum und Klassenzugehörigkeit der Schülerinnen und Schüler verarbeitet. Auch wenn Elternaccounts angelegt werden, müssen hierzu keine Daten der Erziehungsberechtigten importiert werden.

Im Rahmen unserer Öffentlichkeitsarbeit veröffentlichen wir zur Veranschaulichung unserer schulischen Arbeit auf unserer Homepage mit Einwilligung der Mitglieder der Schulgemeinschaft Fotos, Videos und Texte.

Bei der Nutzung schulischer Informationstechnik (z.B. Rechner im Computerraum) werden die Aktivitäten der Nutzerinnen und Nutzer vom Administrator protokolliert. Im Zusammenhang mit der unterrichtsbezogenen Nutzung des landeseigenen pädagogischen Verwaltungsprogramms MNS+ werden Vorname, Name und Geburtsdatum auch an das betreuende IT-Unternehmen übertragen, das einen pseudonymisierten Benutzernamen und ein Passwort zur Anmeldung in MNS+ generiert.

Nutzern ist es durch die verwendete Nextcloud möglich, auch außerhalb des schulinternen Netzes auf bestimmte Bereiche des pädagogischen Verwaltungsnetzes zuzugreifen. Diese wird auf einem städtischen Server betrieben. Alle Lehrerinnen und Lehrer haben jederzeit die Möglichkeit, im schulinternen Netz oder auch über die Nextcloud, auf die Daten der Schülerinnen und Schüler zuzugreifen. Dies erfolgt sowohl im Rahmen der Aufsichts- und Fürsorgepflicht als auch im Rahmen der pädagogischen Arbeit.

Zur Nutzung unseres pädagogischen Netzes mit mobilen Endgeräten stellen wir im Schulgebäude WLAN zur Verfügung.

Unsere Schule nutzt eine Online-Lernplattform des Pädagogisches Landesinstituts Rheinland-Pfalz. Sofern diese Lernplattform auch von Ihrem Kind genutzt wird, werden Sie vorab in einem gesonderten Schreiben über die Datenverarbeitungsvorgänge unterrichtet.

3. An welche Stellen können Daten übermittelt werden?

a. Private und öffentliche Stellen

Unter Beachtung der gesetzlichen Voraussetzungen übermitteln wir Daten beispielsweise an die Schulaufsichtsbehörden, den Schulträger oder an eine andere Schule bei einem Schulwechsel. Wir geben keine Schülerdaten an private Stellen weiter.

b. Auftragsverarbeitung – Drittland

Neben der schuleigenen Nextcloud stellen wir über den OVS-Rahmenvertrag die Nutzung von Microsoft®-Produkten, wie beispielsweise die Cloud OneDrive®, zur Verfügung. Gespeicherte Daten befinden sich auf europäischen Servern. Wir beachten dabei die Vorgaben aus der Datenschutz-Grundverordnung. Um die Nutzung zu ermöglichen, übermitteln wir nur den pseudonymisierten Benutzernamen und das Passwort aus dem pädagogischen Verwaltungsprogramm. Wir empfehlen dennoch, auf dem OneDrive keine persönlichen oder personenbezogenen Daten abzulegen oder zu verwenden..

Das Bildungsministerium hat spezifiziert, dass die datenschutzrechtlichen Bedenken des LfDI zu Produkten von Microsoft sich insbesondere auf den Betrieb der Videokonferenz-Komponente von Teams beziehen, da bei den anfallenden Bild-, Ton- und/oder Verkehrsdaten eine hinreichend starke Verschlüsselung oder Pseudonymisierung im Rahmen von schulischen Nutzungsszenarien aktuell nicht möglich ist. Unter Berücksichtigung der oben genannten Regelung zu Microsoft Teams ist somit nach Gesprächen des Ministeriums für Bildung mit dem LfDI RLP unter bestimmten Voraussetzungen ein Einsatz von Microsoft 365 incl. Teams ohne die Videokonferenz-Komponente im unterrichtlichen Kontext datenschutzrechtlich zulässig. Hierzu zählen zwingend:

- 1) die Nutzung eines Vertragswerks, das auf den aktuellen EU-Standard-Datenschutzklauseln beruht,
- 2) die Verwendung pseudonymer Mailadressen/Accounts für Schülerinnen und Schüler und das Verbot der Nutzung privater Microsoft-Accounts sowie
- 3) die Minimierung des Personenbezugs der beim Lehren und Lernen verarbeiteten Daten.

Diese drei Bedingungen erfüllen wir bereits, weil die Datenschutzklauseln bei Abschluss des FWU-Rahmenvertrages gewährleistet sind, wir nur die pseudonymen Benutzernamen der Schülerinnen und Schüler an Microsoft übertragen und die Schülerinnen und Schüler dazu aufgefordert sind, den One-Drive nur für nicht-personenbezogene Daten und unsere eigene Nextcloud für personenbezogene Daten zu nutzen. Um entsprechend dem dritten Punkt den Personenbezug zu minimieren, legen wir großen Wert darauf, dass unsere Schülerinnen und Schüler bei digitaler Kommunikation nur die Vornamen oder besser nur den Benutzernamen und nicht den gesamten Namen angeben. Zusätzlich deaktivieren

wir das Videokonferenzmodul (auch Audioanrufe) von Teams und stellen der Schulgemeinschaft die Landeslösung BigBlueButton, die in unsere Nextcloud integriert wird, für diese Zwecke zur Verfügung. Eine Kurzanleitung hierzu finden Sie auf der Homepage.

Der schulische Administrator des schulischen Office-Systems kann eine Liste aller von den Benutzern gebildeten Gruppen sowie die zugeordneten Mitglieder einsehen. Die Inhalte der Gruppen können nicht eingesehen werden. Die Nutzung des Office-Systems ist ausschließlich zur schulischen Nutzung gedacht. Dies gilt insbesondere für die Bildung von Gruppen und Teams.

Auch private Gruppen in Office repräsentieren das MSG z.B. durch eine E-Mail-Adresse und sind Teil der schulischen digitalen Lernumgebung. Es ist insbesondere auf eine angemessene Benennung, die die schulische Nutzung erkennen lässt, zu achten. Bei zweifelhafter Benennung kann die Gruppe vom Administrator oder dem Besitzer der Gruppe gelöscht werden.

4. Verhaltensweisen bei der Nutzung von Chats in Teams und Videokonferenzen über BBB

Folgende Verhaltensweisen bei der Nutzung der Chat-Funktion von Teams und der Nutzung von BBB für Videokonferenzen müssen von allen Nutzern beachtet werden:

- Die Chatfunktionen von Teams dürfen nicht missbräuchlich benutzt werden. Insbesondere sind bedrohende und belästigende Anrufe oder Anschreiben zu unterlassen. Die Übermittlung von Informationen mit rechts- oder sittenwidrigen Inhalten oder von Hinweisen auf solche Informationen ist strafrechtlich relevant und nicht erlaubt. Dazu zählen insbesondere Informationen, die im Sinne der §§ 130, 130a und 131 StGB der Volksverhetzung dienen, zu Straftaten anleiten oder Gewalt verherrlichen oder verharmlosen, sexuell anstößig sind, im Sinne des § 184 StGB pornografisch sind oder geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden oder in ihrem Wohl zu beeinträchtigen.
- Zugangsdaten dürfen nicht an Dritte weitergegeben werden und sind vor unberechtigtem Zugriff sicher aufzubewahren. Passwörter sind regelmäßig zu ändern.
- Aufnahmen von Videokonferenzen sind strafbar und zu unterlassen.
- An Videokonferenzen dürfen nur die Schülerinnen und Schüler sowie die Lehrkräfte der jeweiligen Lerngruppe teilnehmen, damit der Unterricht in einem geschützten Rahmen ohne unbefugte Dritte erfolgen kann. Ausnahmen sind bei der Schulleitung zu beantragen.

Bei allen Systemen (BBB, MNS+ mit Nextcloud und Office 365) handelt es sich um digitale, schulische Lernumgebungen, die von einer Administration im Rahmen unserer Aufsichts- und Fürsorgepflicht beaufsichtigt werden. Die Kommunikation der Mitglieder unserer Schulgemeinschaft untereinander kann hierbei von der Administration selbstverständlich nicht eingesehen werden.

Alle Systeme werden für schulische Zwecke bereitgestellt und sollen nicht als private Plattformen verwendet werden.

5. Wie lange werden die Daten gespeichert?

Wir löschen die Daten von Schülerinnen und Schülern grundsätzlich spätestens ein Jahr nach Verlassen der Schule. Für einige Unterlagen bestehen spezielle Aufbewahrungsfristen, z.B. werden Klassen- und Kursbücher sowie Unterlagen über die Lernmittelfreiheit 3 Jahre, Einzelfallakten des Schulpsychologischen Dienstes 5 Jahre, Bafög-Unterlagen 6 Jahre und Abschluss- und Abgangszeugnisse 60 Jahre aufbewahrt.

6. WLAN-Nutzung

Das Max-Slevogt-Gymnasium eröffnet Mitgliedern der Schulgemeinschaft im Bereich des Schulgeländes als freiwilliges Angebot kostenfrei für eingeschränkte Zeiträume über ein Ticketsystem oder ggf. dauerhaft den Zugang zum Internet über ein WLAN, wenn die folgenden Regelungen anerkannt werden.

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

Die Regelungen der Hausordnung bleiben unberührt. Die Lehrkräfte sind berechtigt, für ihren Unterricht Anordnungen zur Nutzung der mobilen Geräte und des Schul-WLAN zu treffen.

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

- Der Zugang zum Internet darf nur für schulische Zwecke genutzt werden. Die gesetzlichen Vorschriften zum Jugendschutzrecht, Urheberrecht und Strafrecht sind zu beachten. Insbesondere dürfen keine Urheberrechte an Filmen, Musikstücken oder Ähnlichem verletzt werden, z.B. durch die Nutzung von Internet-Tauschbörsen. Es ist nicht gestattet, jugendgefährdende, beleidigende, falsche, sexistische, rassistische oder gewaltverherrlichende Inhalte herunterzuladen oder zu verbreiten.
- Der Zugang zum WLAN ist über einen Code aus dem Ticketsystem möglich. Es ist untersagt, diese Daten Dritten zugänglich zu machen; im Zweifelsfall haftet die registrierte Nutzerin/der registrierte Nutzer für unzulässige Aktivitäten Dritter bei der Nutzung seines/ihrer WLAN-Zugangs.
- Nutzungseinschränkungen durch das Vorhandensein von Jugendschutzfiltersoftware der Schule sind zu akzeptieren. Der Versuch, die technischen Filtersperren zu umgehen, kann zum Entzug der Nutzungserlaubnis führen.
- Die Schule übernimmt keine Haftung für die Datensicherheit der von Nutzerinnen und Nutzern genutzten privaten Geräte. Die Verantwortung hierfür liegt ausschließlich bei den Nutzerinnen und Nutzern.
- Jeder Manipulationsversuch an der Netzstruktur wird durch das Max-Slevogt-Gymnasium zur Anzeige gebracht.
- Die Nutzungsaktivitäten der Nutzerinnen und Nutzer werden in Form von MAC-Adressen, die jedem Gerät eindeutig zugeordnet werden können, gemäß der Datenschutzvereinbarung protokolliert und gespeichert. Diese können im Fall der missbräuchlichen Nutzung des Zugangs an Strafverfolgungsbehörden übermittelt

werden. Im Rahmen von Ermittlungsverfahren ist die Schule ggfs. verpflichtet, diese Daten den Ermittlungsbehörden zur Verfügung zu stellen.

- Im Verdachtsfall werden die gespeicherten Protokolldaten ausgewertet. Die Auswertung erfolgt durch von der Schulleitung schriftlich bestimmten Personen.
- Verstöße gegen die Regeln der Nutzerordnung werden durch den Entzug des WLAN-Zuganges und disziplinarische Maßnahmen geahndet und ggf. zur Anzeige gebracht.

7. Nutzung verwalteter iPads

- Alle iPads, die Eigentum der Schule sind, werden über das MDM Jamf School administriert. Im System werden, neben systemspezifischen Daten, selbst installierte Apps (falls möglich), der Ladestand des Akkus, der freie Speicherplatz, MAC-Adresse und Seriennummer, sowie die IP-Adresse, mit der das Gerät mit dem Internet verbunden ist, angezeigt.
- Werden private Geräte in das MDM eingebunden, können zusätzlich die privat installierten Apps angezeigt werden. Daten können nicht eingesehen werden.
- Die Einbindung der schuleigenen und privaten Geräte in das MDM erfolgt ausschließlich unter Verwendung eines pseudonymisierten Benutzernamens.
- iPads von Schülerinnen und Schülern können über die Classroom App auf kurze Distanz begrenzt (Klassenraum) von der im Raum befindlichen Lehrkraft überwacht und gesteuert werden. Dies erfolgt im Rahmen der Aufsichtspflicht und der pädagogischen Arbeit und betrifft in das MDM eingebundene schuleigene und private Geräte.
- Die iPads dürfen von den Schülerinnen und Schülern nur entsprechend der Anweisungen der Lehrkräfte verwendet werden. Bei missbräuchlicher Verwendung kann die Nutzung auch privater Geräte zeitweise untersagt werden.

8. Administration

Neben den externen Dienstleistern Bechtle Mainz und Theile Speyer administrieren die folgenden Personen die schulischen Systeme:

- MNS+ mit angebundenem WLAN und Office 365 werden von Daniel Klein (Stellv. Schulleiter), Anna Seiter (Koordinatorin im digitalen Bereich), Ralf Wagner (Datenschutzbeauftragter) und Marco Kattannek (techn. Assistent) administriert.
- Jamf School wird von Daniel Klein (Stellv. Schulleiter) und Anna Seiter (Koordinatorin im digitalen Bereich) administriert.
- Microsoft 365 wird von Daniel Klein (Stellv. Schulleiter) und Anna Seiter (Koordinatorin im digitalen Bereich) administriert.

9. Welche Datenschutzrechte haben Sie bzw. Ihr Kind?

Nach den Bestimmungen der Datenschutz-Grundverordnung stehen Ihnen bestimmte Datenschutzrechte zu, z.B. das Recht auf Berichtigung oder Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Widerspruchsrecht gegen die Verarbeitung. Außerdem steht Ihnen ein Auskunftsrecht im Hinblick auf die bei uns gespeicherten Informationen über Sie und Ihr Kind zu. Auf Verlangen werden wir Ihnen eine Kopie der personen- bezogenen Daten zur Verfügung stellen. Außerdem können Sie sich bei Beschwerden aus dem Bereich des Datenschutzes an die Schule bzw. den dortigen schulischen Datenschutzbeauftragten sowie an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz wenden.

Landau, 01. August 2024

Stefanie Mehret

Daniel Klein

Dr. Ralf Wagner

Schulleiterin

Stellv. Schulleiter

Datenschutzbeauftragter
