Nutzungsordnung für die IT-Infrastruktur an den Schulen des Kreises Paderborn

1 Allgemeines

1.1 Geltungsbereich

Um eine nachhaltige Nutzung für Sie und Ihre Mitschülerinnen und Mitschüler auch zukünftig gewährleisten zu können, bitten wir Sie die zur Verfügung gestellten Einrichtungen fachgerecht und sorgsam zu nutzen.

Nachfolgende Regelung gilt für die Benutzung von schulischen Computereinrichtungen durch Schülerinnen und Schüler im Rahmen des Unterrichts, der Gremienarbeit und zur Festigung der Medienkompetenz außerhalb des Unterrichts. Sie gilt nicht für die rechnergestützte Schulverwaltung.

Die folgende Nutzungsordnung steckt den Rahmen für eine verantwortungsvolle Nutzung ab.

Die Kenntnisnahme und Einwilligung in diese Regeln sind Voraussetzung für die Erteilung eines Nutzerzugangs. Dabei werden zunächst allgemeine Regeln formuliert (Abschnitt 2) und im zweiten Schritt um spezifische Regeln für die einzelnen IT-Dienste (Abschnitt 3) ergänzt.

1.2 Laufzeit

Dem Benutzer wird innerhalb seiner Dienstzeit/Schulzeit Zugang zur pädagogischen IT-Infrastruktur der Schule gewährt. Diese Zugangsgewährung endet automatisch mit dem Tag des Verlassens der Schule.

1.3 Zuwiderhandlungen

Im Falle von Verstößen gegen diese Nutzungsordnung oder deren Beihilfe behält sich die Schulleitung das Recht vor, die Nutzung einzelner oder aller IT-Dienste zu untersagen. Davon unberührt behält sich die Schulleitung weitere dienstrechtliche Maßnahmen oder Ordnungsmaßnahmen vor.

1.4 Umfang

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhalten Sie Zugang zu verschiedenen IT-Systemen:

- zum pädagogischen Netz unserer Schule
- zu unserer Arbeitsplattform Office 365 ProPlus (im Folgenden „Office 365“).

2 Regeln für jede Nutzung

2.1 Passwörter

- Für jeden durch die Schule angebotenen IT-Dienst müssen unterschiedliche Passwörter verwendet werden. Es darf kein Passwort mehrmals verwendet werden.
- Soweit aktiviert, sollte die 2-Faktor-Authentifizierung genutzt werden.
- Die Passwörter müssen sicher sein und dürfen nicht erratbar sein. Sie müssen aus **mindestens 8 Zeichen** bestehen, worunter sich **Zahlen**, **Groß- und Kleinbuchstaben** und **Sonderzeichen** befinden müssen.
- Die Passwörter sollten nicht in den bekannten Passwortdatenbanken vorkommen. Das ist bspw. hier zu prüfen: https://haveibeenpwned.com/Passwords.

- Die Passwörter dürfen nicht an Dritte weitergegeben werden. Ein Passwort muss sofort geändert werden, sobald es die Vermutung gibt, dass Fremde Kenntnis vom Passwort bekommen haben.
- Die Nutzung eines lokalen Passwortmanagers ist zu empfehlen.
- Weitere Informationen zum Umgang mit Passwörtern finden Sie hier: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html

2.2 Zugangsdaten

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

2.3 Eingriffe in die Hard- und Softwareinstallation

Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerkes sowie Manipulationen an der Hardwareausstattung sind grundsätzlich untersagt. Geräte dürfen nur mit Zustimmung der aufsichtführenden Person an Computer oder an das Netzwerk angeschlossen werden.

2.4 Schutz der Geräte

Die Bedienung der Hard- und Software hat stets sachgerecht zu erfolgen. Störungen oder Schäden sind sofort der für die Computernutzung verantwortlichen Person zu melden. Wer schuldhaft Schäden verursacht, hat diese zu ersetzen.

2.5 Unzulässige Inhalte und Handlungen

Benutzer sind verpflichtet, bei der Nutzung der durch die Schule angebotenen IT-Dienste geltendes Recht einzuhalten.

- Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte abzurufen, zu speichern oder zu verbreiten.
- Die geltenden Jugendschutzvorschriften sind zu beachten.
- Die Verbreitung und das Versenden von belästigenden, verleumderischen oder bedrohenden Inhalten ist unzulässig.
- Die von der Schule bereitgestellten IT-Dienste dürfen nicht für die Versendung von Massen-Nachrichten (Spam) und/oder anderen Formen unzulässiger Werbung genutzt werden.
- Es dürfen keine unberechtigten Downloads von Musikdateien, Spielen etc. durchgeführt werden.
- Es dürfen keine Tauschbörsen genutzt werden.
- Es darf nicht an Gewinnspielen teilgenommen werden.
- Es dürfen keine kostenpflichtigen Onlinespiele gespielt werden.
- Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (z.B. Videos) aus dem Internet, ist verboten, solange keine schulischen Gründe vorliegen.

- Es dürfen keine nicht unterrichtsbezogenen Dateien im schulischen Netzwerk gespeichert werden.

2.6 Urheberrecht

- Bei der Nutzung der durch die Schule angebotenen IT-Dienste 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 den durch die Schule angebotenen IT-Dienste 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 zur Verfügung gestellten digitalen Inhalten von Lehrmittelverlagen ist das Urheberrecht zu beachten. Eine Nutzung ist nur innerhalb der schulischen IT-Dienste zulässig. Nur wenn die Nutzungsbedingungen der Lehrmittelverlage es gestatten, ist eine Veröffentlichung oder Weitergabe digitaler Inhalten von Lehrmittelverlagen zulässig.
- Stoßen Benutzer in den durch die Schule angebotenen IT-Dienste 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 den durch die Schule angebotenen IT-Dienste unberührt.

2.7 Datenschutz und Datensicherheit

- Die Schule ist in Wahrnehmung ihrer Aufsichtspflicht berechtigt, den Datenverkehr zu speichern und zu kontrollieren.
- Die Schule wird von ihren Einsichtsrechten nur in Fällen des Verdachts von Missbrauch und durch verdachtsunabhängige Stichproben Gebrauch machen.
- Es dürfen keine personenbezogenen Daten Dritter (z.B. Name, Geburtsdatum, Personenfotos) im Internet veröffentlicht werden. Die Speicherung dieser Daten ist auf allen Geräten zu minimieren.

3 Regeln für einzelne IT-Dienste

3.1 Pädagogischer Account (SNV)

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhält der Schüler/ die Schülerin Zugang zum pädagogischen Netz (Schulnetzverwalter=SNV) der Schule.

Alle berechtigten Schülerinnen und Schüler erhalten für den Zugang zu den Computersystemen der Schule und zum schulischen Netzwerk jeweils eine individuelle Nutzerkennung und wählen sich ein Passwort (Zugangsdaten). Mit diesen Zugangsdaten können sie sich an allen zugangsgesicherten Computersystemen der Schule anmelden. Das Computersystem, an dem sich ein Nutzer im Netz angemeldet hat, ist aus Sicherheitsgründen durch diesen niemals unbeaufsichtigt zu lassen. Nach Beendigung der Nutzung hat sich der Nutzer an seinem Computersystem ordnungsgemäß abzumelden.

Schüler/innen nutzen das pädagogische Netz nur zur Datenablage unterrichtlicher Inhalte. Dafür steht ihnen ein eigenes Verzeichnis zur Verfügung. Damit die Lehrkräfte Unterrichtsmaterial verteilen und oder einsammeln können, haben diese Zugriff auf die Verzeichnisse der Schüler/innen.

3.2 Schul-Mailing

Für Schulen ist und bleibt E-Mail eine wichtige Möglichkeit, Informationen zu übermitteln, innerhalb der Schule wie auch nach außen. E-Mails sind im Prinzip vergleichbar zu Postkarten, wenn sie nicht durch entsprechende Maßnahmen geschützt werden. Das bedeutet, derart transportierte Informationen sind auf dem Weg zum Empfänger offen einsehbar für jedermann, der in der Lage ist, sie unterwegs abzufangen, sei es auf dem Weg vom Absender zum Server seines E-Mail Anbieters, auf dem Server selbst, wie auf dem weiteren Weg. Allgemeine Informationen, die keine personenbezogenen Daten enthalten oder „Betriebsgeheimnisse“ wie Entwürfe für Prüfungen oder ähnlich, können problemlos vollkommen ungesichert versandt werden, auch von privaten E-Mail-Konten. Sobald es jedoch um personenbezogene Daten geht, ist das absolut nicht mehr möglich.

Im Folgenden sind alltagstaugliche Möglichkeiten aufgezeigt, wie die Übermittlung von personenbezogenen Daten per E-Mail absichert werden kann.

- Nutzen Sie kein privates E-Mail Konto, um personenbezogene Daten aus der Schule zu übermitteln.
- Sichern Sie Ihren Computer, von welchem aus Sie E-Mails versenden (ob über Webmailer oder Client) immer vor fremden Zugriffen durch Personen oder Schadsoftware (Viren, Trojaner) ab.
- Schützen Sie den Zugang zu Ihrem E-Mail Konto immer durch ein sicheres Passwort.
- Versenden Sie personenbezogene Daten niemals per E-Mail ohne Schutzmaßnahmen außer Sie kommunizieren innerhalb einer E-Mail Domain und nutzen dabei den Zugang über den Webmailer und achten auf eine sichere Verbindung. Nutzen Sie alternativ einen E-Mail Client als Zugang, müssen Sie sicherstellen, dass die Verbindung im Client sicher eingestellt ist.
- Leiten Sie E-Mails mit personenbezogenen Daten aus einem dienstlichen E-Mail Konto niemals auf eine private E-Mail Adresse weiter.
- Wenn Sie nicht in der Lage sind, E-Mails selbst zu verschlüsseln, packen Sie die zu übermittelnden Inhalte in eine Datei oder einen Ordner, welchen Sie in ein durch sicheres Passwort und Verschlüsselung geschütztes ZIP Archiv umwandeln und so vor unberechtigter Kenntnisnahme schützen. Das Passwort, teilen Sie dem Empfänger auf anderem Wege, z.B. telefonisch mit.
- Arbeiten Sie mit Microsoft Office, können Sie Word und Excel Dateien mit einem Passwort vor unberechtigter Kenntnisnahme schützen und die Datei so per E-Mail versenden. Das Passwort übermitteln Sie getrennt, möglichst auf einem anderen Weg, z.B. telefonisch.

3.3 Office 365, insbesondere MS Teams, OneNote, Forms, OneDrive, Sharepoint

3.3.1 Geltungsbereich

Die Berufskollegs stellen den Schülerinnen und Schülern neben einem Benutzerkonto im pädagogischen Netzwerk eine Lizenz ‚Office 365 A1 Plus für Schüler und Studenten‘ zur Verfügung. Diese beinhaltet

- den Zugang zum Online-Portal Microsoft Office 365
- Onlinespeicher (Microsoft OneDrive)
- eine schulische E-Mail-Adresse
- das Recht, die aktuelle Version der Office-Anwendungen MS Word, MS Excel, MS PowerPoint, MS OneNote sowie MS Teams lokal auf bis zu fünf Geräten (PC, Laptop, Tablet, Smartphone)

gleichzeitig zu installieren. Microsoft hat dabei das Recht, die Anwendungen fortlaufend weiterzuentwickeln.

Beim Verlassen der Schule wird das Benutzerkonto deaktiviert und gelöscht sowie die Zuweisung der Office 365 Lizenz aufgehoben.

Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, der Arbeitsplattform Office 365 sowie den eigenen personenbezogenen Daten und denen von anderen in der Schule lernenden und arbeitenden Personen voraus. Die folgende Nutzungsvereinbarung informiert und steckt den Rahmen ab für eine verantwortungsvolle Nutzung und ihre Annahme bzw. die Einwilligung sind Voraussetzung für die Erteilung eines Nutzerzugangs.

3.3.2 Datenschutz und Datensicherheit

Mit Microsoft wurde zur Nutzung von Office 365 ein Vertrag abgeschlossen, welcher gewährleistet, dass personenbezogene Daten von Benutzern nur entsprechend der Vertragsbestimmungen verarbeitet werden.

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

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

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

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

3.3.3 E-Mail

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

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

3.3.4 Kalender

Die Aufnahme von privaten, nicht schulischen Terminen (z.B. Geburtstagen) in den Kalender von Office 365 ist nicht zulässig.

3.3.5 Kopplung mit privaten Konten oder anderen Diensten

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

3.4 Digitale Klassenbuch

3.4.1 Was ist das Elektronischen Klassenbuchs (EKB)?

Das EKB (WebUntis) erlaubt Lehrkräften und Schüler/innen einen webbasierten Zugriff auf den eigenen tagesaktuellen Stundenplan. Diese Daten werden bei jeder Vertretungsplanänderung aktualisiert. Außerdem lassen sich die Unterrichtsinhalte der Unterrichtsstunden einsehen. Außerdem verwalten die Klassenleitungen mit dem EKB die Abwesenheitszeiten der Schüler ihrer Klasse.

3.4.2 Wie kann ich das EKB nutzen?

Am einfachsten über die kostenlose Untis-App, die über den Google Play Store oder den Apple App Store erhältlich ist. Auch über die Webseite mese.webuntis.com ist eine Anmeldung möglich. Für die Anmeldung erhalten Sie von der Schule einen Benutzernamen und ein Kennwort, mit dem Sie beim Server anmelden können. Die persönlichen Anmeldedaten dürfen nicht weitergereicht werden.

3.5 Moodle (LEBK)

3.5.1 Was ist Moodle

Die MOODLE-Lernplattform ist ein komplexes E-Learningsystem, dass der Bereitstellung von Lerninhalten und der Organisation von Lernvorgängen in Kursen dient. Es umfasst alle Lernbereiche, vom Meinungsaustausch unter den Lernenden bis hin zur Bewertung von Lernergebnissen.

3.5.2 Wie kann ich Moodle nutzen

Um an den verschiedenen Kursen teilnehmen zu können, müssen Sie sich einen Nutzerzugang für diese Website anlegen. Für einige Kurse könnte zusätzlich ein Zugangsschlüssel notwendig sein, dass Ihnen der Lehrende/Trainer mitteilt. Details zum Anlegen eines Benutzerkontos, die Einschreibung in die unterschiedlichen Kurse und Hinweise zum Datenschutz finden Sie auf der Website unter: https://lebk.lms.schulon.org/login/index.php

3.6 Private Geräte (BYOD)

Die Nutzung von privaten Geräten zu schulischen Zwecken ist erlaubt, solange die folgenden Voraussetzungen gegeben sind.

- Die Internetverbindung erfolgt über das schulische Netzwerk ausschließlich über das zur Verfügung gestellte WLAN mit der SSID xxxx_S.
- Die auf dem privaten Gerät installierte Software, insbesondere das Betriebssystem ist auf dem aktuellen Stand zu halten. Alle aktuellen Sicherheitsupdates müssen installiert sein.
- Die privaten Geräte sind nach dem aktuellen Stand der Technik abgesichert (z.B. Anti-Virensoftware).
- Die privaten Geräte sind immer lautlos einzustellen. Im Unterricht sind Kopfhörer zu tragen, sollten Medien mit einer Audiospur verwendet werden.

4 Ergänzende Regeln für die Nutzung außerhalb des Unterrichtes

4.1 Selbstlernphasen

Außerhalb des Unterrichts kann im Rahmen der medienpädagogischen Arbeit ein Nutzungsrecht in ausgewiesenen Räumen (z.B. Selbstlernzentren oder Mediatheken) gewährt werden. Die Entscheidung darüber und welche Dienste genutzt werden können, trifft die Schule unter Beteiligung der schulischen Gremien.

Alle Nutzer werden über diese Nutzungsordnung unterrichtet. Die Schülerinnen und Schülerinnen sowie im Falle der Minderjährigkeit ihre Erziehungsberechtigten, versichern durch ihre Unterschrift (siehe Anlage), dass sie diese Ordnung anerkennen. Dies ist Voraussetzung für die Nutzung.

5 Schlussvorschriften

Nutzer, die unbefugt Software von den Arbeitsstationen oder aus dem Netz kopieren oder verbotene Inhalte nutzen, machen sich strafbar und können zivil- oder strafrechtlich verfolgt werden.

Einmal zu jedem Schuljahresbeginn findet eine Nutzerbelehrung statt, die im Klassenbuch protokolliert wird.

Datenschutzrechtliche Informationen nach Art. 13 DS-GVO

Zur Nutzung der verschiedenen IT-Dienste an der **[Schulname]** ist die Verarbeitung von personenbezogenen Daten erforderlich. Darüber möchten wir Sie/ Euch im Folgenden informieren.

Konkret geht es um die folgenden IT-Dienste, die nicht zustimmungspflichtig sind:

- Pädagogisches Netz (SNV)
- Lernplattform (moodle)

Sowie den weiteren IT-Diensten, deren Nutzung zustimmungspflichtig ist:

- Eigener Account zum Digitalen Klassenbuch (Webuntis)
- Office 365
- Bring Your Own Device

Im Folgenden wird jeder IT-Dienst einzeln in Bezug auf die Verarbeitung von personenbezogenen Daten aufgezählt.

1 Datenverarbeitende Stelle

Kontaktdaten Schule	***Schulischer Datenschutzbeauftragter***
Ludwig-Erhard-Berufskolleg des Kreises Paderborn	*Manfred Bergmann*
Schulleiterin OStD‘ Christiane Menne	*Schulamt für den Kreis Paderborn*
Schützenweg 4	*Rathenaustr. 96*
33102 Paderborn	*33102 Paderborn*
E-Mail: info@lebk.de	*E-Mail: bergmannm@schulamt-paderborn.de*

2 Pädagogisches Netz (SNV)

5.1 Wofür werden personenbezogene Daten verarbeitet?

Der Schulnetzverwalter (SNV) ist eine Klassenraum-Management-Software mit pädagogischer Oberfläche und integrierter Benutzerverwaltung.

5.2 Warum dürfen personenbezogene Daten verarbeitet werden?

Rechtsgrundlage für die Datenverarbeitung ist § 120 Absatz 5 Schulgesetz NRW in Verbindung mit Artikel 6 Absatz 1 lit. e) DSGVO und § 3 Absatz 1 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW).

5.3 Welche personenbezogenen Daten werden verarbeitet und wer ist davon betroffen?

- **Anmeldeinformationen** (Nutzerkennung, Passwort, Passworthinweis)

- **Nutzerinhalte** (erzeugte Dateien und Inhalte, Versionen von Dateien)
- **technische Daten** (Datum, Zeit, Gerät, Traffic, IP Nummern aufgesuchter Internetseiten und genutzter Dienste)
- **Geräte-Identifikationsdaten** (Gerätename, MAC Adresse), bei BYOD

5.4 Wer hat Zugriff auf die personenbezogenen Daten?

5.4.1 Intern:

- **Lehrkräfte, andere Benutzer/ Schüler** (nur gemeinsame Daten oder von Nutzern in ein gemeinsames Verzeichnis übermittelte Daten oder Freigaben),
- **Administratoren** (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich),
- **Schulleitung** (alle technischen und öffentlichen Daten, Daten im persönlichen Nutzerverzeichnis nur im begründeten Verdachtsfall einer Straftat oder bei offensichtlichem Verstoß gegen die Nutzungsvereinbarung),

5.4.2 Extern:

- **Dienstleister, Administratoren** (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich, auf Weisung der Schulleitung)
- **Ermittlungsbehörden** (alle Daten betroffener Nutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- **Betroffene** (Auskunftsrecht nach Art. 15 DS-GVO)

5.5 Wann werden die personenbezogenen Daten wieder gelöscht?

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 gelöscht. Bis dahin ist es für den Benutzer möglich, sich die Inhalte des persönlichen Verzeichnisses aushändigen zu lassen.

6 Lernplattform (moodle)

6.1 Wofür werden personenbezogene Daten verarbeitet?

Unsere MOODLE-Lernplattform ist ein komplexes E-Learningsystem, dass der Bereitstellung von Lerninhalten und der Organisation von Lernvorgängen dient. Es umfasst alle Lernbereiche, vom Meinungsaustausch unter den Lernenden bis hin zur Bewertung von Lernergebnissen.

Damit das reibungslos funktioniert werden durch die Software eine Reihe von Daten über Sie gespeichert.

6.2 Warum dürfen personenbezogene Daten verarbeitet werden?

Rechtsgrundlage für die Datenverarbeitung ist § 120 Absatz 5 Schulgesetz NRW in Verbindung mit Artikel 6 Absatz 1 lit. e) DSGVO und § 3 Absatz 1 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW).

6.3 Welche personenbezogenen Daten werden verarbeitet und wer ist davon betroffen?

Von MOODLE gespeicherte personenbezogene Daten:

- Name, Vorname
- Benutzername

- Klasse-, Kurszugehörigkeit
- E-Mail-Adresse
- Zugriffszeit, Inhalt, IP-Adresse
- Protokolldaten über Abgaben,
- Beiträge in Foren, Wikis, Abgaben,
- Testergebnisse
- Bewertungen

6.4 Wer hat Zugriff auf die personenbezogenen Daten?

Ihre Profildaten sowie Ihre Forumseinträge können alle Teilnehmer Ihres Kurses aufrufen. Ihre nichtöffentlichen Eingaben, (Abgaben, Testantworten, Logdaten) können nur vom jeweiligen Kursleiter eingesehen und ausgewertet werden.

Alle Daten obliegen der Verschwiegenheitspflicht der Lehrpersonen und werden weder an Dritte innerhalb der Schule noch außerhalb der Schule weitergegeben.

6.5 Wann werden die personenbezogenen Daten wieder gelöscht?

Die Kursdaten werden spätestens 4 Wochen nach Beendigung des Kurses gelöscht, Logdaten nach 14 Tagen. Ihr Moodlekonto wird 1 Jahr nach Ablauf des Kalenderjahres gelöscht, in dem Sie die Ausbildung beendet haben.

6.6 Was mache ich, wenn ich Fehler in den Daten finde und wenn kann ich bei Fragen kontaktieren?

Sollten Sie Fehler in Ihren Daten feststellen, wenden Sie sich bitte an Leiter des Kurses oder an den Administrator der Moodle-Instanz. Diese werden helfen, die Fehler in den Daten zu korrigieren. Sie können sich aber auch an den zuständigen Datenschutzbeauftragten wenden.

Die Kontaktdaten für diese Lernplattform entnehmen Sie bitte dem Impressum der Seite.

6.7 Werden weitere Daten in meinem Browser gespeichert?

Die Moodle-Website benutzt zwei Cookies. Cookies sind kleine Datenpakete, welche zwischen Computerprogrammen ausgetauscht werden, um den Nutzer zu identifizieren.

1. MoodleSession: Sie müssen dieses Cookie erlauben, damit der Login bei allen Moodle-Zugriffen von Seite zu Seite erhalten bleibt. Nach dem Ausloggen oder dem Schließen des Webbrowsers wird das Cookie gelöscht.
2. MoodleID: Dieses Cookie dient der Bequemlichkeit. Es speichert den Anmeldenamen im Webbrowser. Dieses Cookie bleibt auch nach dem Ausloggen aus Moodle erhalten. Beim nächsten Login ist dann der Anmeldename bereits eingetragen.

7 Digitales Klassenbuch (Webuntis)

7.1 Wofür werden personenbezogene Daten verarbeitet?

Die Daten werden benötigt, um ein personalisiertes Benutzerkonto für Sie anzulegen. Dieses ermöglicht es Ihnen, Ihren tagesaktuellen Stundenplan und die Unterrichtsinhalte der Unterrichtsstunden einzusehen.

7.2 Warum dürfen personenbezogene Daten verarbeitet werden?

Die Verarbeitung personenbezogener Daten bei Nutzung von Webuntis erfolgt auf der Grundlage von DS-GVO Art. 6 lit. a (Einwilligung).

7.3 Welche personenbezogenen Daten werden verarbeitet und wer ist davon betroffen?

Name, Vorname und Geburtsdatum

7.4 Wer hat Zugriff auf die personenbezogenen Daten?

Auf personenbezogene Daten hat nur der jeweilige Schüler, die jeweilige Klassenleitung und die Bildungsgangleitung Zugriff.

7.5 Wann werden die personenbezogenen Daten wieder gelöscht?

Das Nutzerkonto wird nach Ausscheiden aus der Schule gelöscht.

8 Office 365

8.1 Wofür werden personenbezogene Daten verarbeitet?

Personenbezogene Daten der Benutzer von 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.

8.2 Warum dürfen personenbezogene Daten verarbeitet werden?

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

8.3 Welche personenbezogenen Daten werden verarbeitet und wer ist davon betroffen?

- **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 Office 365 Pro Plus)
- Diese Daten werden sowohl für Schülerinnen und Schüler als auch von Lehrkräften erhoben.

8.4 Wer hat Zugriff auf die personenbezogenen Daten?

8.4.1 Intern:

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

8.4.2 Extern:

- **Microsoft** (zur Bereitstellung der Dienste von 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)

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

- **Ermittlungsbehörden** (alle Daten betroffener Benutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- **Betroffene** (Auskunftsrecht nach Art. 15 DS-GVO)

8.5 Werden meine Daten außerhalb der EU verarbeitet?

Bei der Nutzung von MS Teams können auch Daten auf Servern in den USA verarbeitet werden. Dabei geht um Daten, welche dazu dienen, die Sicherheit und Funktion der Plattform zu gewährleisten und zu verbessern. Wir haben mit dem Anbieter von MS Teams einen Auftragsverarbeitungsvertrag geschlossen, der den Anforderungen von Art. 28 DSGVO entspricht. Ein angemessenes Datenschutzniveau ist durch den Abschluss der sog. EU-Standardvertragsklauseln garantiert.

8.6 Wann werden die personenbezogenen Daten wieder gelöscht?

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

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

Benutzer müssen ihre Daten vorher eigenständig sichern.

9 Recht auf Widerruf

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

10 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.

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