Grundschule und Mittelschule Asbach-Bäumenheim

Microsoft 365
Nutzungsvereinbarung

Grund- und Mittelschule Asbach-Bäumenheim

Josef-Dunau-Ring 4
86663 Asbach-Bäumenheim

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhältst du/ erhalten Sie Zugang zur Arbeitsplattform Microsoft 365 Education (ehemals Office 365, und im Folgenden „Microsoft 365“). Den Zugang zu Microsoft 365 stellen wir dir/Ihnen auch außerhalb des Unterrichts zur schulischen Nutzung zur Verfügung. Die Nutzung setzt einen verantwortungsvollen Umgang mit der Arbeitsplattform Microsoft 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. Ihre Annahme bzw. die Einwilligung sind Voraussetzung für die Erteilung eines Nutzerzugangs.

Inhalt

Grundschule und Mittelschule Asbach-Bäumenheim

Nutzungsvereinbarung:

Geltungsbereich

Die Nutzungsvereinbarung gilt für Schüler und Lehrkräfte, nachfolgend "Benutzer" genannt, welche Microsoft 365 zur elektronischen Datenverarbeitung nutzen.

Umfang

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

- Die Möglichkeit die Microsoft 365 Apps (ehemals Office) auf bis zu 5 Privatgeräten zu installieren, im Rahmen der durch die Schule erworbenen Microsoft 365 A5 Lizenz

- Zugang zu Microsoft 365 mit
  - einer schulischen E-Mail-Adresse (Microsoft Exchange Online)
  - Online-Speicherplatz auf Microsoft OneDrive
  - Online-Klassenlaufwerke auf Microsoft SharePoint
  - Microsoft 365 Apps (Word, Excel, PowerPoint, OneNote, Teams)

- Anmeldung an Bestands- und Leihgeräten für Schüler
  - mit einer schulischen E-Mail-Adresse
  - zur Durchführung von Arbeiten innerhalb der Unterrichtszeiten in- und außerhalb des Schulgebäudes
  - welche verwaltet und dokumentiert werden, durch die Schule und Administration bzw. durch die Microsoft Geräte-Verwaltungsinstanz Microsoft Intune

Grundschule und Mittelschule Asbach-Bäumenheim

Datenschutz und Datensicherheit

Die Schule sorgt mitsamt einer umfangreichen Microsoft Lizenzierung durch technische und organisatorische Maßnahmen für den Schutz und die Sicherheit der im pädagogischen Netz verarbeiteten personenbezogenen Daten, die weit über dem üblichen Maße hinausgehen.

Mit Microsoft wurde zur Nutzung von Microsoft 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 Microsoft 365 nicht zur Erstellung von Profilen zur Anzeige von Werbung oder Direkt-Marketing zu nutzen.

Ziel unserer Schule ist es, durch eine Minimierung von personenbezogenen Daten bei der Nutzung von Microsoft 365 auf das mindeste 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 beitragen und auch das Recht anderer Personen an der Schule auf informationelle Selbstbestimmung respektieren.

Hierfür ist auch ein verantwortungsvolles und sicheres Handeln von Wichtigkeit, welches zum Schutze der Benutzer auch durch technische Implementierungen mitunter erzwungen wird.

Passwörter

- müssen sicher und nicht erratbar sein. Sie müssen aus mindestens 8 Zeichen bestehen worunter sich eine Zahl, ein Groß- und Kleinbuchstabe und ein Sonderzeichen befinden müssen.
- sollten zumindest einmal im Schuljahr gewechselt werden.
- zusätzlich wird die Anmeldung mit dem Passwort durch eine Multi-Faktor-Authentifizierung mit der „Microsoft Authenticator“-App ergänzt, um das Konto vor Zugriffen oder Angriffen durch leicht zu erratende oder gestohlene Kennwörter zu schützen.

Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum persönlichen Microsoft 365 Konto geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben werden.
- Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist der Benutzer verpflichtet, ist das Zugangspasswort selbstständig zu ändern. Im Regelfall ist dies jedem Benutzer selbstständig am Schulgerät oder auf einer beliebigen Microsoft Webseite möglich. Für Ausnahmefälle 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 bzw. Leihgerät meldet sich der Benutzer des pädagogischen Netzes ab (ausloggen oder herunterfahren).

Gerätenutzung

- Die Schule stellt Schülern zur Durchführung Ihrer Arbeiten im pädagogischen Netz Arbeitsstationen in den IT-Räumen bereit.
- Darüber hinaus ist die Möglichkeit gegeben, nach vorheriger Absprache, Leihgeräte mit Nachhause zu nehmen, um damit den schulischen Tätigkeiten nachzugehen.
- Je nach Vereinbarung können über einen vereinbarten Zeitraum auch schulisch verwaltete iPads überlassen werden.
- Relevante Benutzerverzeichnisse (Desktop, Bilder, Dokumente) werden nach Anmeldung des Benutzers am Gerät automatisch mit Microsoft OneDrive synchronisiert. Dadurch sind die Daten des Benutzers jederzeit an jedem Gerät oder über die Webdienste Microsofts in einem einheitlichen Stand verfügbar.
- Benutzerdaten, die auf dem Gerät abgelegt oder durch Microsoft OneDrive synchronisiert werden, sind durch Windows Bitlocker zu jeder Zeit verschlüsselt.
- Benutzerdaten werden automatisch von einem Gerät gelöscht, sofern der Benutzer sich nicht am gleichen Gerät innerhalb 60 Tage angemeldet hat. Sollte der Speicherplatz des Gerätes verknappen, kann eine Löschung früher erfolgen.
  In beiden Fällen sind die Daten des Benutzers weiterhin im persönlichen Microsoft OneDrive vorhanden, und werden nach einer kurzen Zeitspanne nach Anmeldung am Gerät wieder synchronisiert.
- Die Gerätenutzung für Schüler ist durch die Geräteverwaltung stark eingeschränkt, sodass die Installation eigener Programme, oder der Zugriff auf nicht zulässige Inhalte blockiert wird.
- Die Mitnahme und USB-Sticks zum Zwecke der Datenspeicherung von Dokumenten ist möglich, jedoch werden sämtliche ausführbaren Inhalte blockiert und in vollem Umfang (hinsichtlich Skriptausführung) dokumentiert und automatisiert gemeldet.
- Trotz Möglichkeiten der USB-Stick Verwendung sollte dies nur den Ausnahmefall darstellen, da sich Benutzer mit einer hinterlegten Multi-Faktor-Authentifizierungsmethode zu jeder Zeit über einen beliebigen Browser sicher authentifizieren und über onedrive.com auf ihre persönlichen Inhalte zugreifen können. Auch die Verwendung der OneDrive App auf einem Mobilgerät für den Datenzugriff ist möglich.

Personenbezogene Daten

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

Exchange Online (E-Mail und Kalender)

Bestandteil des Microsoft 365 Paketes ist die Microsoft Exchange Online Funktionalität, die dem Benutzer eine schulische E-Mail-Adresse bereitstellt.

- Die Nutzung des schulischen E-Mail-Kontos ist **nur für schulische Zwecke** zulässig. Die E-Mail-Adresse wird benötigt für die Anmeldung in den Microsoft Applikationen und an den schulischen Geräten.
- Wie bei den anderen Komponenten von Microsoft 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**. Eingerichtete automatische Weiterleitungen an Adressen außerhalb der Schule werden blockiert und gemeldet.
- Die Aufnahme von privaten, nicht schulischen Terminen in den Kalender von Office 365 **ist nicht zulässig**, sofern der Termin nicht als „Privat“ gekennzeichnet wurde. Für die Kennzeichnung ist eine entsprechende Schaltfläche zur Markierung vorhanden, welche bei Erstellung des Termins ausgewählt werden kann.
- Das Einpflegen von Geburtstagen im schulischen Kalender sollte zwecks Übersichtlichkeit vermieden werden.
- Personenbezogene bzw. private Dateianhänge an Kalenderterminen sind zu vermeiden.

SharePoint

Zur Erfüllung der schulischen Bildungsmaßnahmen gilt es im Unterricht, Schülern innerhalb der Kurse bzw. Klassen Unterrichtsdokumente zu verteilen. Die Verteilung erfolgt dabei über Microsoft SharePoint, das als Online-Klassenlaufwerk fungiert.

Über eine Verknüpfung auf dem Desktop der Schulgeräte wird der Benutzer zum SharePoint Portal weitergeleitet und kann auf die durch die Lehrkraft geteilten Inhalte seines Kurses bzw. Klasse Einsicht nehmen. Das Hochladen von Dokumenten durch den Benutzer in das Klassenlaufwerk ist möglich, und wird beispielsweise zur Abgabe von Gruppenarbeiten oder Präsentationen nötig sein.
Aufgrund der gemeinsamen Nutzung gilt es sich an die Regeln der gemeinsamen Nutzung zu halten.

- Das Hochladen von privaten bzw. personenbezogenen Inhalten ist zu vermeiden, sofern dies nicht dem Unterricht dienlich ist oder durch eine Lehrkraft angefordert wird.
- Das Hochladen von Inhalten, die das Klassenklima stören könnten, ist untersagt.
- Löschung von Inhalten, die durch den Benutzer fälschlicherweise hochgeladen wurden ist gestattet. Die Inhalte von Klassenkameraden gilt es zu respektieren und nicht zu löschen.
- Die Inhalte können durch eine Lehrkraft ohne Vorankündigung geändert oder gelöscht werden.
- Im Regelfall erfolgt das Leeren des Klassenlaufwerks zum Wechsel des Schuljahres. Wichtige Dokumente sollte der Benutzer daher in seinem persönlichen OneDrive Speicher sichern, z.B.: durch Speichern des Dokuments auf dem Desktop eines Schulgeräts für die Synchronisation mit dem Benutzerkonto.

OneDrive

Im Rahmen der Microsoft 365 A5 Lizenz steht dem Benutzer bis zu 5TB (5000 Gigabyte) Speicherplatz für seine persönlichen Daten zur Verfügung. Um eine unsachgemäße Verwendung solch großen Speicherplatzes zu verhindern, wurde der Speicherplatz für eine Schule übliche Größe eingeschränkt.

- Der belegte Speicherplatz kann durch den Benutzer über die Microsoft OneDrive Webseite oder über die auf den Geräten installierte Microsoft OneDrive Applikation eingesehen werden.
- Sollte der Speicherplatz nicht ausreichen, kann nach Absprache und Betrachtung der bisherigen Inhalte mit einer Lehrkraft der Speicherplatz im Rahmen einer Ausnahmeregelung für den Benutzer durch die Administration erhöht werden.
- Für die OneDrive Inhalte ist der Benutzer selbst verantwortlich.
- Gelöschte oder veränderte OneDrive Inhalte können selbstständig durch den Benutzer wiederhergestellt werden über die Papierkorb Funktionalität bzw. über den Versionsverlauf. Typischerweise ist der Verlauf über einen Rechtsklick auf die Datei über das Untermenü OneDrive zu erreichen.
- Die OneDrive Daten des Benutzers bleiben im Regelfall bis zum Austritt aus der Schule erhalten.

Microsoft Teams

Die Verwendung von Microsoft Teams wird im Rahmen der schulischen Verwendung gestattet. Kommunikationen mit Kontakten außerhalb der Schule sind gesperrt.

- Die Nutzung von Microsoft Teams ist nur zum schulischen Austausch zulässig, oder zur Unterstützung und effizienteren Erreichung der geplanten Lernziele.
- Die Nutzung von Microsoft Teams in Form der mobilen Applikation ist ebenfalls zulässig, gemeinsam mit der Möglichkeit mit anderen Mitschülern bzw. Mitbenutzern über Teams zu telefonieren oder Konferenzen zu führen.
- Da Microsoft Teams im technischen Hintergrund mitunter auf Exchange Online und SharePoint aufbaut, gelten einzelne Beschränkungen aus den vorherigen Passagen auch für diesen Dienst.
- Inhalte, die im Microsoft Teams Chat versendet werden, werden im persönlichen OneDrive Order des Benutzers gespeichert, die die Datei versendet hat.
- Kanalinhalte werden hingegen zentral gespeichert, sodass diese bei Schulaustritt weiterhin bis zur Bereinigung verbleiben können, sofern für diese ein Bedarf besteht.
- Die Verwendungsmöglichkeiten von Microsoft Teams sind innerhalb einer Konferenz oder einem geplanten Termin eingeschränkt, um den Organisator des Termins oder den Unterrichtsfluss nicht zu stören.
- Sollte die missbräuchliche Verwendung von Microsoft Teams festgestellt werden, wird dem Benutzer die Zugriffsmöglichkeit auf allen Geräten entzogen, und bedeutet unter Umständen, dass Unterrichtsmaterialen ggf. auf anderem Wege bereitgestellt werden.

Kopplung mit privaten Konten oder anderen Diensten

- Zur Wahrung des Schutzes und der Sicherheit der eigenen personenbezogenen Daten ist es nicht möglich, das schulische Microsoft 365 Konto mit anderen privaten Konten von Microsoft oder anderen Anbietern zu koppeln. Eine solche Kopplung wird seitens Schule blockiert.
- Eine Nutzung des schulischen Microsoft 365 Kontos zur Authentifizierung an anderen Online-Diensten ist nicht zulässig und blockiert, außer es ist ein von der Schule zugelassener Dienst.
- Anmeldung an den schulischen Geräten oder Inhalten mit anderen privaten Microsoft Konten ist nicht möglich und erfordert stets das persönliche schulische Konto.
- Die Geräte sind an die schulische Organisation mitsamt der Hardwareadresse gebunden, sodass im Falle eines Diebstahles die Bindung weiter bestehen bleibt und die Fremdverwendung unterbunden wird. Für die erneute Einrichtung ist zwingend ein Benutzer der schulischen Organisation erforderlich.
- Sollte das Gerät im Rahmen einer Ausgliederung für den dauerhaften privaten Besitz überlassen werden, muss dies zunächst zurückgesetzt und die Bindung durch administrative Austragung aus dem Inventar aufgehoben werden. Andernfalls ist die Verwendung auch nach einer vollständigen Formatierung und Neuinstallation von Windows nicht möglich.

Datenlöschung

- Grundsätzlich wird bei Schulaustritt des Benutzers die Microsoft 365 A5 Lizenz entzogen, und das Benutzerkonto zur Löschung markiert, womit der Zugriff auf das Benutzerkonto nicht länger möglich ist. Auf privaten Geräten installierte Microsoft 365 Apps (ehemals Microsoft Office, z.B.: Word, Excel, PowerPoint) können nicht länger verwendet werden und müssen, sofern keine andere Lizenz oder ein privates lizenziertes Microsoft-Konto vorliegt, deinstalliert werden. Nach 30 Tagen werden sämtliche Benutzerinformationen aus Microsoft 365 entfernt, einschließlich aller Microsoft Exchange Online (E-Mail, Kalender) und Microsoft OneDrive (persönliche Daten) Inhalte. Eine Wiederherstellung des Benutzers und der Inhalte ist nach Ablauf der Frist nicht mehr möglich. Gegebenenfalls können Restbestände in den zentralen schulischen Datensicherungen vorliegen, die automatisch zum Ablauf der technischen Vorhaltefrist bereinigt werden. Die Möglichkeit zur vorzeitigen Löschung solcher Inhalte befindet sich in der technischen Planungsphase.
- Bei einem vorzeitigen Austritt gelten dieselben Fristen, mit Ausnahme von Inhalten aus Microsoft SharePoint (Klassenlaufwerke), die ggf. bis zum Schuljahreswechsel erhalten bleiben können. Darüber hinaus werden im Nachfolgenden Einzelausnahmen definiert.
- Die Inhalte in Microsoft SharePoint (Klassenlaufwerke) können ohne Vorankündigung durch eine Lehrkraft oder einen Administrator teilweise oder im Ganzen gelöscht werden. Im Regelfall werden die Inhalte, sofern nicht anderweitig angekündigt, zum Schuljahreswechsel vollständig gelöscht. Die Verwaltung der Klassenlaufwerksinhalte obliegt im Regelfall den Lehrkräften.
- Die Inhalte im persönlichen Microsoft OneDrive können durch den jeweiligen Benutzer ergänzt, verändert oder jederzeit gelöscht werden. Die Ablage von Dokumenten ist dem Benutzer freigestellt, sofern diese nicht gegen Vorgaben der Schule verstoßen. Die Verwaltung der Microsoft OneDrive Inhalte obliegt im Regelfall dem jeweiligen Benutzer.
- Die Inhalte in Microsoft Exchange Online (E-Mail und Kalender) können durch den jeweiligen Benutzer innerhalb seines Postfachs ergänzt, verändert oder gelöscht werden. Auch ein E-Mail-Versand oder die Erstellung von privat gekennzeichneten Terminen ist möglich, sofern dies nicht gegen Vorgaben der Schule verstoßen.
- Die Inhalte auf den schulischen Geräten werden automatisch nach 60 Tagen bereinigt, sofern innerhalb der Zeitspanne keine Anmeldung durch den Benutzer am jeweiligen Gerät stattgefunden hat. In Ausnahmefällen kann eine Löschung früher erfolgen, wenn der belegte Speicher des Gerätes einen Schwellwert überschreitet. Die Daten aus dem persönlichen OneDrive des Benutzers sind nicht von der Löschung betroffen, da bei der Verwendung des Gerätes nur Kopien der Daten synchronisiert werden.
- Auf die Inhalte des Benutzers aus Microsoft SharePoint, Microsoft OneDrive, Microsoft Exchange Online, und die der Schulgeräte können bei Verdacht auf Missbrauch oder unsachgemäßer Verwendung durch einen Administrator Einsicht genommen werden. Auch eine Löschung und Meldung entsprechender Inhalte ist nicht ausgeschlossen.

Urheberrecht

- Bei der Nutzung von Microsoft 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 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 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 und Lernprodukte bei einer Veröffentlichung entsprechend der ursprünglichen Creative Commons Lizenzen zu lizenzieren.
- Bei von der Schule über Microsoft 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 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 365 unberührt.

Unzulässige Inhalte und Handlungen

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

- Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über das pädagogische Netz und Microsoft 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 365 darf nicht für die Versendung von Massen-Nachrichten (Spam) und/oder anderen Formen unzulässiger Werbung genutzt werden.

Zuwiderhandlungen

Im Falle von Verstößen gegen diese Nutzungsordnung behält sich die Schulleitung das Recht vor, den Zugang zu einzelnen oder allen Bereichen innerhalb des pädagogischen Netzes und von Microsoft 365 zu sperren. Davon unberührt behält sich die Schulleitung weitere dienstrechtliche Maßnahmen, Ordnungsmaßnahmen oder im Falle von Sicherheitsgefährdungen an die zuständige Datenschutzhörde vor.

Weiterführende technische Sicherheitsmaßnahmen

In Zeiten der steigenden Angriffe und Identitätsgefährdungen ist es nicht länger ausreichend, auf herkömmliche Schutzmaßnahmen und einen Basis-Antivirenschutz zu setzen. Daher wendet die Schule weitgehende automatisierte kostenpflichtige KI-basierte Analysen für unterschiedliche Szenarien hinsichtlich der Verhaltensweise der Anmeldungen, Geräte, Applikationen und Verbindungen an, die von diesen aus erfolgen.

- Die Verwendung der Geräte wird nicht nur mithilfe der Verwaltungsinstanz Microsoft Intune eingeschränkt und auf Konformität geprüft, sondern durch weitere Dienste und Abhängigkeiten KI-basiert automatisiert geschützt.
- Jedes Schulgerät wird als einzelne isolierte Instanz geführt, damit zentrale Infektionen über herkömmliche Wege unterbunden werden.
- Ausgeführte oder heruntergeladene Anwendungen und Dateien werden mithilfe von Windows Smartscreen auf unerwünschte Inhalte geprüft, und durch Microsoft Defender for Endpoint neben einer signaturbasierten Prüfung zudem KI-basiert im Verhalten analysiert, um ggf. gefährliche Handlungsmuster zu erkennen, zu melden, und weitere Geräte und Benutzer der Schule zu schützen, bevor ein Angriff stattfinden kann.
- Durchgeführte oder versuchte Angriffe werden automatisiert ausführlich protokolliert und analysiert, womit der Angriff über mehrere Geräte, Verbindungen und Wochen hinweg auf den einzelnen Benutzer mitsamt Inhalten der durchgeführten Schritte zurückgeführt werden kann.
- Aufgerufene Webseiten werden durch Microsoft Defender for Endpoint auf unerlaubt Kategorien geprüft und ggf. blockiert.
- Aufgebaute verschlüsselte Internetverbindungen (SSL/TLS) durch Anwendungen auf den Schulgeräten werden im Zweifelsfall aufgebrochen, die Inhalte analysiert und bei Bedarf blockiert.
- Anmeldungen an den Geräten oder an den Microsoft Diensten werden neben der Prüfung der Zugangsdaten und den Authentifizierungsmerkmalen zudem auf KI-basiert abweichende Anmeldemuster und Anmeldeverhalten geprüft, die im Einzelfall in einzelne Risikostufen eingeordnet werden. Je nach Risikostufe kann entweder eine zusätzliche Authentifizierung erfordert werden oder das Konto gemeldet, gesperrt und eine Passwortänderung zur Freischaltung erforderlich sein. Alle weiteren verbundenen Geräte erfordern eine erneute Bestätigung der Sitzung.
- Versendete und empfangene Links und Anhänge in Microsoft Teams werden aufgelöst, und auf Schädlichkeit geprüft, bevor diese dem Empfänger zur Verfügung gestellt werden. Gegebenenfalls werden schädliche Inhalte bereinigt und entfernt, oder sofern keine alternative Aktion zur Verfügung steht, gänzlich blockiert.
- Versendete und empfangene Links und Anhänge in Exchange Online (und die damit verbundene Verwendung von Microsoft Outlook) werden bei Empfang zunächst in einer isolierten Form ohne Anhang mit einem Hinweis dargestellt, dass der Anhang nach Prüfung bereitgestellt wird. Nach Abschluss der Prüfung wird die E-Mail automatisch durch das freigegebene Original im Postfach des Empfängers ersetzt.
- Aufgrund der Null-Toleranz-Vorgehensweise hinsichtlich der Sicherheit werden unbekannte Plattformen, Applikationen, Zugriffsmuster oder gefährliche Aktionen erkannt, analysiert und pauschal blockiert. Zugriffe auf jedwede Ressource aus dem Ausland sind deaktiviert.

Nutzungsbedingungen von Microsoft

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.