

Nutzungsordnung für die Verwendung des bereitgestellten schulischen Microsoft 365 Education Accounts

1. Worum handelt es sich bei Microsoft 365 Education?

Die Schule stellt für das gemeinsame Arbeiten und Lernen im Unterricht und zuhause Microsoft 365 Education zur Verfügung. Diese Software ermöglicht den Schülern und den Lehrkräften, auch bei räumlicher Distanz, eng zusammenzuarbeiten und zu kommunizieren. Nachfolgende Regelungen bilden den Rahmen für eine verantwortungsvolle Nutzung von Microsoft 365 Education.

Mit der Nutzung von Microsoft 365 Education verpflichten Sie sich, diese Regelungen einzuhalten.

2. Was beinhaltet Microsoft 365 Education?

Mit den Diensten, Programmen und Apps können Sie mit Lehrkräften und anderen Schülerinnen und Schülern im Unterricht zusammenarbeiten. Die Programme, Dienste und Apps können Sie auch zu Hause zum Lernen und Arbeiten für die Schule verwenden.

Beinhaltet sind:

- Microsoft 365 Apps (früher Office 365 ProPlus genannt) für die lokale Installation auf bis zu 10 privaten Geräten (PC, Mac, Tablet Smartphone)
- Upgrade auf Windows 10 Education für bis zu 5 private Geräte
- Nutzung der Onlineversionen der gängigen Microsoft 365 Apps auf allen Endgeräten
- Cloud-Speicher mit 1 Terabyte Speicherplatz
- persönliche schulische E-Mail-Adresse (vorname.nachname@s.bszmw.de).
- Plattform für Chat und Videokonferenz
- Kollaborationsplattform (ermöglicht gemeinsame zeitgleiche Arbeit an Dokumenten, Teamarbeit)

3. Voraussetzung zur Verwendung von Microsoft 365 Education und Nutzungszeitraum

Eine Nutzung von Microsoft 365 Education ist nur möglich, wenn die Nutzerinnen/der Nutzer ihre/seine schriftliche **Einwilligung** erklären. Bei minderjährigen Schülerinnen und Schülern ist die Einwilligung der Erziehungsberechtigten erforderlich. Bei Minderjährigen zwischen 14 und 18 Jahren ist zusätzlich zur Einwilligung der Erziehungsberechtigten die eigene Zustimmung erforderlich.

Sie dürfen Microsoft 365 Education so lange verwenden wie Sie einer Schule des BSZ zugehören. Wenn Sie die Schule verlassen oder Microsoft 365 Education nicht mehr benutzen möchten, wird Ihr Konto nach einer kurzen Übergangsfrist gelöscht. Dann können Sie auch keine Dienste, Programme und Apps mehr nutzen. Wir behalten uns vor, nach Ablauf eines jeden Schuljahres Ihre Gruppenmitgliedschaften (Teams und SharePoint) und deren Inhalte zu löschen. Zu Beginn eines jeden Schuljahres werden neue Teams erstellt. Das Sichern Ihrer Dateien und Daten liegt in Ihrer eigenen Verantwortung.

4. An welche Regeln muss ich mich halten?

Sie sind verpflichtet sich bei der Nutzung von Microsoft 365 Education an das geltende Recht zu halten. Nehmen Sie keine unrechtmäßigen Handlungen vor.

Beachten Sie insbesondere folgende Punkte:

- a) Die Nutzung der Plattform ist nur für schulische Zwecke zulässig. Das Speichern von privaten Dateien (z.B. private Bilder und Videos) ist auf der zur Verfügung gestellten Cloud („OneDrive“) nicht erlaubt.
- b) Sie sind verpflichtet, bei der Nutzung der Plattform geltendes Recht einzuhalten, u. a. das Strafrecht und das Jugendschutzrecht
- c) Verletzen Sie keine Rechte anderer und halten Sie sich an die Regeln des Urheberrechts. Fremde Inhalte (Texte, Fotos, Videos, Lieder, Audio und andere Materialien) dürfen Sie nicht ohne Genehmigung der Urheber in Microsoft 365 Education speichern. Dazu gehören auch eingescannte oder abfotografierte Texte und Bilder.
- d) Unterlassen Sie es, unangemessene Inhalte oder anderes Material (das z. B. Nacktdarstellungen, Brutalität, Pornografie, anstößige Sprache, Gewaltdarstellungen oder kriminelle Handlungen oder deren Aufruf zum Inhalt hat) zu veröffentlichen oder über die Dienste zu teilen.
- e) Die Verbreitung und das Versenden von extremistischen, rassistischen, diskriminierenden, belästigenden, beleidigenden oder bedrohenden Inhalten sind verboten.
- f) Sie dürfen keine Massen-Nachrichten (Spam) und/oder anderen Formen unzulässiger Werbung versenden.
- g) Unterlassen Sie Handlungen, die betrügerisch, falsch oder irreführend sind (z. B. sich als jemand anderes ausgeben oder versuchen die Dienste zu manipulieren).
- h) Unterlassen Sie es, wissentlich Beschränkungen des Zugriffs auf bzw. der Verfügbarkeit der Programme und Apps zu umgehen.
- i) Unterlassen Sie Handlungen, die Ihnen oder anderen Schaden zufügen (z. B. das Übertragen von Viren).
- j) Unterlassen Sie Handlungen, die die Privatsphäre von anderen verletzen. Von den Teilnehmerinnen und Teilnehmern über die Plattform bereitgestellte Inhalte dürfen nicht unbefugt in sozialen Netzwerken verbreitet werden.
- k) Es ist jede Nutzung untersagt, die geeignet ist, die berechtigten Interessen der Schule zu beeinträchtigen (z. B. Schädigung des öffentlichen Ansehens der Schule; Schädigung der Sicherheit der IT-Ausstattung der Schule).
- l) Helfen Sie niemandem bei einem Verstoß gegen diese Regeln

5. Was passiert, wenn ich mich nicht an die Regeln halte?

Bei Regelverstößen kann die Schulleitung Ihren Zugang zu Microsoft 365 Education sperren lassen. Die Schulleitung behält sich vor weitere schulische Ordnungsmaßnahmen gegen Sie zu verhängen oder in besonders schweren Fällen rechtliche Schritte einzuleiten.

6. Erreichbarkeit der Lehrkräfte

Die Lehrkräfte sind im Allgemeinen zu den üblichen Dienstzeiten über ihre dienstliche E-Mail erreichbar. Wir streben eine zeitnahe Beantwortung an. Dies kann aber aufgrund unterschiedlicher Tätigkeitsbereiche einer Lehrkraft nicht immer taggleich gewährleistet werden.

7. Wie ist es mit dem Schutz und Sicherheit meiner (personenbezogenen) Daten?

Um für Schülerinnen, Schülern und Lehrkräften die benötigten Nutzerkonten zu erstellen, werden personenbezogene Daten an den Dienstleister DrVis Software GmbH sowie Microsoft Ireland Operations, Ltd. übermittelt. Folgende persönliche Daten werden bei Erstellung des Benutzerkontos verarbeitet:

- Benutzername (vorname.nachname@bszwmw.de)
- Schulzugehörigkeit
- Zugehörigkeit zu Klasse, Fächern und ggf. Kursen.

Nähere Informationen sind der Anlage „Informationen zur Datenverarbeitung nach Art. 13 DSGVO“ zu entnehmen.

Beachten Sie weiterhin:

- Je weniger persönliche Daten Sie bei der Nutzung von Microsoft 365 oder anderen Diensten von sich herausgeben und je verantwortungsvoller Sie handeln, desto besser können Sie zum Schutz und zur Sicherheit Ihrer personenbezogenen Daten beitragen.
- Respektieren Sie auch das Recht anderer Personen an der Schule auf deren informationelle Selbstbestimmung. Die Aufzeichnung einer Bild-, Ton- oder Videoübertragung, z. B. durch eine Software oder das Abfotografieren des Bildschirms, ist nicht gestattet.
- Die Kamera- und Tonfreigabe durch die Nutzerinnen und Nutzer erfolgt freiwillig. Wir empfehlen die Kamera nicht zu aktivieren. Bitte beachten Sie, dass es nicht ausgeschlossen werden kann, dass Dritte, die sich mit Nutzerinnen und Nutzern im selben Zimmer befinden, z.B. Haushaltsangehörige, den Bildschirm einer Nutzerin oder eines Nutzers und darauf abgebildete Kommunikationen einsehen können.
- Personenbezogene Daten (z.B. Lebensläufe, Klassenfotos, Filme, etc.) gehören grundsätzlich nicht in die Microsoft Cloud, weder die eigenen noch die von anderen.
- Sensible Daten gem. Art. 9 DSGVO (z. B. Gesundheitsdaten, rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetischen und biometrischen Daten) dürfen nicht verarbeitet werden.
- Bei der Nutzung sind das Mithören und die Einsichtnahme durch Unbefugte zu vermeiden. Die Nutzung der Videokonferenzfunktionen an öffentlichen Orten, insbesondere in öffentlichen Verkehrsmitteln, ist untersagt.
- Im Rahmen des Unterrichts kann es jedoch vorkommen, dass personenbezogene Daten entstehen. Bei Ihren personenbezogenen Daten und bei denen von anderen haben Sie dafür zu sorgen, dass Sicherheit und Schutz von personenbezogenen Daten nicht durch leichtsinniges, fahrlässiges oder vorsätzliches Handeln gefährdet werden.
- Daher sind solche Daten nur in Ausnahmefällen (Genehmigung der Lehrkraft) und nach dem Prinzip der Datenminimierung und Datensparsamkeit sowie in verschlüsselter Form abzuspeichern.
- Eine Verwendung des schulischen Nutzerkontos zur Authentifizierung an anderen Online-Diensten ist nicht zulässig, außer es ist ein von der Schule zugelassener Dienst.
- Wenn Sie weitere Fragen haben, wende Sie sich bitte an Ihre Lehrkraft oder an den Datenschutzbeauftragten oder die Datenschutzbeauftragte der Schule.

7.1 Was muss ich bezüglich meiner Zugangsdaten beachten?

- Ihr Passwort muss sicher sein und darf nicht einfach erratbar sein. Ihr Passwort muss aus mindestens 8 Zeichen bestehen, worunter sich eine Zahl, ein Großbuchstabe und ein Sonderzeichen befinden müssen.
- Sie sind verpflichtet, die eigenen Zugangsdaten zum persönlichen Microsoft 365 Education Konto geheim zu halten und dürfen diese nicht an andere Personen weitergeben.
- Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, sind Sie verpflichtet, sofort Maßnahmen zum Schutz des eigenen Zugangs zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist der schulische Administrator zu informieren.
- Sollten Sie in Kenntnis fremder Zugangsdaten gelangen, so ist es Ihnen untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Sie sind jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.
- Nach Ende der Unterrichtsstunde bzw. bei Verlassen Ihres Arbeitsplatzes müssen Sie sich von Ihrer aktuellen Microsoft 365 Education Sitzung abmelden (**ausloggen!**).
- Beim Einsatz mobiler (privater) Geräte müssen diese mindestens durch eine PIN oder ein Passwort geschützt werden.

7.2 Können meine Aktivitäten bei Microsoft 365 Education überwacht oder kontrolliert werden?

Wenn Sie die Dienste, Programme und Apps verwenden, werden Ihre Aktivitäten automatisch erfasst und gespeichert. Man bezeichnet dieses Protokollieren als «Loggen». Dies ist z. B. auch notwendig, damit Benutzer unerwünschte Änderungen rückgängig machen können. Die Protokolldaten dürfen nur bearbeitet werden, wenn dies für das Funktionieren des Systems notwendig ist. Sollte der Verdacht eines Missbrauchs der Dienste durch Benutzer vorliegen, können Protokolldaten unter Hinzuziehung des örtlichen Datenschutzbeauftragten ausgewertet werden. Die Betroffenen werden entsprechend informiert (siehe auch Punkt 5).