Nutzungsordnung zur Nutzung der IT-Infrastruktur und des Internetzugangs an der Schönwerth-Realschule Amberg

A. Allgemeiner Teil

I. Allgemeines und Geltungsbereich

Die Schönwerth-Realschule Amberg gibt sich für die Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs sowie für die Nutzung von im Verantwortungsbereich der Schule stehenden Cloudangeboten (einschließlich digitaler Kommunikations- und Kollaborationswerkzeuge) folgende Nutzungsordnung. Sie gilt für Schülerinnen und Schüler, Lehrkräfte und sonstiges an der Schule tätiges Personal.

Teil A der Nutzungsordnung trifft allgemeine Vorschriften für alle Nutzerinnen und Nutzer, Teil B sieht besondere Vorschriften für Schülerinnen und Schüler vor und Teil C enthält besondere Vorschriften, die nur für Lehrkräfte und sonstiges an der Schule tätiges Personal gelten.

II. Regeln für jede Nutzung

1. Allgemeine Regeln

Die schulische IT-Infrastruktur darf nur verantwortungsvoll und rechtmäßig genutzt werden. Insbesondere sind die Vorgaben des Urheberrechts und die gesetzlichen Anforderungen an Datenschutz und Datensicherheit zu beachten.

Persönliche Zugangsdaten müssen geheim gehalten werden. Die Verwendung von starken, d. h. sicheren Passwörtern wird empfohlen. Detaillierte Empfehlungen zu Länge und Komplexität von Passwörtern finden sich auf der Homepage des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Bei Verdacht, dass Zugangsdaten bekannt geworden sind, muss das entsprechende Passwort geändert werden. Das Arbeiten unter fremden Zugangsdaten sowie die Weitergabe des Passworts an Dritte ist verboten.

Bei der Konfiguration sind weitere Sicherheitsvorkehrungen wie z.B. Verzögerungen, IP-Sperren im erforderlichen Umfang zu berücksichtigen.

Es dürfen keine Versuche unternommen werden, technische Sicherheitsvorkehrungen wie Webfilter oder Passwortschutz zu umgehen.

Auffälligkeiten, die die Datensicherheit betreffen, müssen an den Datenschutzbeauftragten der Schule Herrn StR (RS) Markus Braun (markus.braun@schoenwerth-Realschule.de; 09621 915650) gemeldet werden. Dies betrifft insbesondere öffentlich gewordene Passwörter oder falsche Zugangsberechtigungen.

2. Eingriffe in die Hard- und Softwareinstallation

Der unerlaubte Eingriff in die Hard- und Softwareinstallation und -konfiguration ist verboten. Dies gilt nicht, wenn Veränderungen auf Anordnung des Systembetreuers oder des Schulleiters durchgeführt werden oder wenn temporäre Veränderungen im Rahmen des Unterrichts explizit vorgesehen sind.

Private Endgeräte und externe Speichermedien dürfen nur mit Zustimmung einer Lehrkraft oder einer Aufsicht führenden Person an die schulische IT-Infrastruktur oder das Schulnetz angeschlossen werden.

3. Anmeldung an den schulischen Endgeräten im Unterrichtsnetz

Die Nutzung der schulischen Endgeräte sowie des Internetzugangs an diesen Geräten ist ohne individuelle Authentifizierung möglich. Zur Nutzung des schulischen WLAN und bestimmter Dienste (z. B. Cloudangebote, Lernplattform, Microsoft 365 etc.) ist eine Anmeldung mit Benutzernamen und Passwort erforderlich.

Nach Beendigung der Nutzung haben sich die Nutzerinnen und Nutzer abzumelden.

4. Anmeldung im Verwaltungsnetz

Im Verwaltungsnetz werden besonders schützenswerte Daten verarbeitet. Daher ist eine benutzerspezifische Authentifizierung mit Benutzername und Passwort notwendig.

Die Berechtigungen werden nach Maßgabe von Aufgaben und Erfüllung schulischer Zwecke verteilt.

5. Protokollierung der Aktivitäten im Schulnetz

Es findet keine regelmäßige Protokollierung der Aktivitäten der Schülerinnen und Schüler sowie der Lehrkräfte und des sonstigen an der Schule tätigen Personals innerhalb des Schulnetzes statt. Es ist der Systembetreuung in Absprache mit der Schulleitung dennoch aus begründetem Anlass gestattet, vorübergehend eine Protokollierung zu technischen Zwecken durchzuführen, z. B. zur Erkennung von Bandbreitenengpässen, der Überprüfung der Funktionsfähigkeit des Schulnetzes oder der Sicherheitsanalyse der schulischen IT-Infrastruktur, vgl. Art. 6 Abs. 1 S.1 lit. e) DSGVO i. V. m. Art. 85 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG).

Die dadurch erzeugten Daten werden nach Abschluss der Analysen unwiderruflich gelöscht.

6. Private Nutzung der schulischen IT-Infrastruktur

Den Lehrkräften und sonstigem an der Schule tätigen Personal ist es gestattet, die schulische IT-Infrastruktur (z. B. Internetzugang, Drucker) außerhalb des Unterrichts und anderen Lernzeiten in geringem Umfang zu privaten Zwecken zu nutzen, z. B. zum Abruf von privaten Nachrichten oder zur privaten Recherche auf Webseiten. Nicht erlaubt ist es, über den schulischen Internetzugang größere Downloads für private Zwecke durchzuführen. Ein Anspruch auf Privatnutzung besteht nicht. Bei Missachtung der Nutzungsordnung oder anderweitigem Fehlverhalten kann das Recht auf Privatnutzung entzogen werden.

Jede Nutzerin bzw. jeder Nutzer ist selbst dafür verantwortlich, dass keine privaten Daten auf schulischen Endgeräten zurückbleiben.

7. Verbotene Nutzungen

Die rechtlichen Bestimmungen – insbesondere des Strafrechts, des Urheberrechts, des Datenschutzrechts und des Jugendschutzrechts – sind zu beachten. Es ist insbesondere verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen, zu speichern oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist beim Aufruf durch Schülerinnen und Schüler der Aufsicht führenden Person umgehend Mitteilung zu machen und anschließend die Anwendung unverzüglich zu schließen.

8. Besondere Verhaltensregeln im Distanzunterricht

Im Distanzunterricht sind bestimmte Verhaltensregeln zu beachten, um einen störungsfreien Unterricht sicherzustellen. Insbesondere beim Einsatz eines digitalen Kommunikationswerkzeugs sind geeignete Vorkehrungen gegen ein Mithören und die Einsichtnahme durch Unbefugte in Video- oder Telefonkonferenz, Chat oder E-Mail zu treffen, vgl. die vom Staatsministerium für Unterricht und Kultus (Staatsministerium) zur Verfügung gestellten Hinweise, abrufbar unter www.km.bayern.de/schule-digital/datensicherheit-an-schulen.html.

Zum Schutz der Persönlichkeitsrechte anderer Nutzerinnen und Nutzer ist zu gewährleisten, dass die Teilnahme oder Einsichtnahme unbefugter Dritter ausgeschlossen ist. Für die Anwesenheit von Erziehungsberechtigten, der Schulbegleitung, von Ausbilderinnen und Ausbildern, Kolleginnen und Kollegen oder sonstigen Personen in Videokonferenzen gilt: Soweit diese nicht zur Unterstützung aus technischen, medizinischen oder vergleichbaren Gründen benötigt werden und auch sonstige Gegebenheiten ihre Anwesenheit nicht zwingend erfordern (z. B. kein separater Raum für den Distanzunterricht, Aufsichtspflicht), ist ihre Beteiligung nicht zulässig.

9. Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs mit privaten Endgeräten

Die Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs mit privaten Endgeräten ist gestattet.

III. Nutzungsbedingungen für den Internetzugang über das schulische WLAN

Die folgenden Ausführungen gelten sinngemäß – soweit anwendbar – auch für Konstellationen, in denen sich die Nutzerinnen und Nutzer über LAN mit dem Netz verbinden.

1. Gestattung zur Nutzung des kabellosen Internetzugangs (WLAN)

Die Schönwerth-Realschule stellt einen kabellosen Internetzugang (WLAN) zur Verfügung. Sie bietet der jeweiligen Nutzerin bzw. dem jeweiligen Nutzer für die Dauer des Aufenthaltes die Möglichkeit einer Mitbenutzung des Internetzugangs der Schule über WLAN. Dies gilt grundsätzlich unabhängig davon, ob der Zugriff über schulische oder private Geräte erfolgt.

Die Nutzerin bzw. der Nutzer ist nicht berechtigt, Dritten die Nutzung dieses WLANs zu gestatten. Die zur Verfügung gestellte Bandbreite ist begrenzt. Es besteht kein Anspruch auf tatsächliche Verfügbarkeit, Geeignetheit und Zuverlässigkeit des Internetzugangs.

Die Schönwerth-Realschule ist aus gegebenem Anlass jederzeit berechtigt, den Zugang der Nutzerin bzw. des Nutzers teil- oder zeitweise zu beschränken oder sie bzw. ihn von einer weiteren Nutzung ganz auszuschließen.

2. Zugang zum schulischen WLAN

Individueller Zugang zum schulischen WLAN über Benutzername und Passwort

Die Anmeldung am WLAN erfolgt über persönliche Zugangsdaten, die der Nutzerin bzw. dem Nutzer von der Schule zur Verfügung gestellt werden (Zugangssicherung). Diese Zugangsdaten dürfen nicht an Dritte weitergegeben werden und sind geheim zu halten. Die Schule kann diese Zugangsdaten jederzeit ändern bzw. in ihrer Gültigkeit zeitlich beschränken. Bei Ungültigkeit der Zugangsdaten können neue Zugangsdaten angefordert werden. Die Zugangsdaten erstrecken sich auf das Internet und auf die von der Schule für die Nutzerin bzw. den Nutzer zur Verfügung gestellten Ressourcen (z. B. Microsoft 365).

3. Haftungsbeschränkung

Die Nutzung des schulischen WLANs erfolgt auf eigene Gefahr und auf eigenes Risiko der Nutzerin bzw. des Nutzers. Für Schäden an privaten Endgeräten oder Daten der Nutzerin bzw. des Nutzers, die durch die Nutzung des WLANs entstehen, übernimmt die Schule keine Haftung, es sei denn, die Schäden wurden von der Schule vorsätzlich oder grob fahrlässig verursacht.

Der unter Nutzung des schulischen WLANs hergestellte Datenverkehr verwendet eine Verschlüsselung nach dem aktuellen Sicherheitsstandard, so dass die missbräuchliche Nutzung Dritter so gut wie ausgeschlossen ist und die Daten nicht durch Dritte eingesehen werden können.

Die Schule setzt geeignete Sicherheitsmaßnahmen ein, die dazu dienen, Aufrufe von jugendgefährdenden Inhalten oder das Herunterladen von Schadsoftware zu vermeiden. Dies stellt aber keinen vollständigen Schutz dar. Die Sicherheitsmaßnahmen dürfen nicht bewusst umgangen werden.

4. Verantwortlichkeit der Nutzerin bzw. des Nutzers

Für die über das schulische WLAN übermittelten Daten sowie die darüber in Anspruch genommenen Dienstleistungen und getätigten Rechtsgeschäfte ist die Nutzerin bzw. der Nutzer allein verantwortlich und hat etwaige daraus resultierende Kosten zu tragen.

Die Nutzerin bzw. der Nutzer ist verpflichtet, bei Nutzung des schulischen WLANs geltendes Recht einzuhalten. Insbesondere ist die Nutzerin bzw. der Nutzer dazu verpflichtet,

- keine urheberrechtlich geschützten Werke widerrechtlich zu vervielfältigen, zu verbreiten oder öffentlich zugänglich zu machen; dies gilt insbesondere im Zusammenhang mit der Nutzung von Streamingdiensten, dem Up- und Download bei Filesharing-Programmen oder ähnlichen Angeboten;
- keine sitten- oder rechtswidrigen Inhalte abzurufen oder zu verbreiten;
- geltende Jugend- und Datenschutzvorschriften zu beachten;

- keine herabwürdigenden, verleumderischen oder bedrohenden Inhalte zu versenden oder zu verbreiten („Netiquette“);
- das WLAN nicht zur Versendung von Spam oder Formen unzulässiger Werbung oder Schad-Software zu nutzen.

5. Freistellung des Betreibers von Ansprüchen Dritter

Die Nutzerin bzw. der Nutzer stellt den Bereitsteller des Internetzugangs von sämtlichen Schäden und Ansprüchen Dritter frei, die auf eine rechtswidrige Verwendung des schulischen WLANs durch die Nutzerin bzw. den Nutzer oder auf einen Verstoß gegen die vorliegende Nutzungsordnung zurückzuführen sind. Diese Freistellung erstreckt sich auch auf die mit der Inanspruchnahme bzw. deren Abwehr zusammenhängenden Kosten und Aufwendungen.

6. Protokollierung

Bei der Nutzung des schulischen Internetzugangs wird aus technischen Gründen die IP-Adresse des benutzten Endgeräts erfasst.

Die Aktivitäten der einzelnen Nutzerinnen und Nutzer bei Nutzung des schulischen Internetzugangs werden grundsätzlich protokolliert. Es ist der Systembetreuung in Absprache mit der Schulleitung bzw. dem Schulaufwandsträger aus begründetem Anlass gestattet, vorübergehend eine Auswertung der Protokollierungsdaten z. B. zu technischen Zwecken durchzuführen.

IV. Verantwortungsbereiche

Die Verantwortungsbereiche der einzelnen Gruppe der Schulgemeinschaft bei der Nutzung der IT-Infrastruktur der Schule und des Internetzugangs und die entsprechenden Rechte, Pflichten und Aufgaben sind wie folgt geregelt:

1. Verantwortungsbereich der Schulleitung

Die Schulleitung ist dazu verpflichtet, eine Nutzungsordnung zu erlassen. Sie hat die Systembetreuung, den Betreuer oder die Betreuerin des Internetauftritts der Schule, die Lehrkräfte sowie weitere Aufsicht führende Personen, sonstiges an der Schule tätiges Personal sowie die Schülerinnen und Schüler über die Geltung der Nutzungsordnung und deren Inhalt zu informieren. Insbesondere hat sie dafür zu sorgen, dass die Nutzungsordnung an dem Ort, an dem Bekanntmachungen der Schule üblicherweise erfolgen, angebracht bzw. abgelegt wird. Die Schulleitung hat die Einhaltung der Nutzungsordnung zumindest stichprobenartig zu überprüfen. Die Schulleitung ist ferner dafür verantwortlich, dass bei einer Nutzung der schulischen IT-Infrastruktur und des Internetzugangs eine ausreichende Aufsicht sichergestellt ist. Sie hat die dafür erforderlichen organisatorischen Maßnahmen zu treffen.

Aufgrund der datenschutzrechtlichen Verantwortlichkeit der Schule hat die Schulleitung, unterstützt durch die zuständige Datenschutzbeauftragte bzw. den zuständigen Datenschutzbeauftragten, die Einhaltung der datenschutzrechtlichen Bestimmungen durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

2. Verantwortungsbereich der Systembetreuung

Der Systembetreuer berät die Schulleitung zusammen mit dem Datenschutzbeauftragten bei der konkreten Gestaltung und Nutzung der schulischen IT-Infrastruktur und des Internetzugangs sowie der Abstimmung mit dem zuständigen Schulaufwandsträger. Der Systembetreuer regelt und überprüft die Umsetzung folgender Aufgaben:

- Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs/WLANs (Zugang mit oder ohne individuelle Authentifizierung, klassenbezogener Zugang),
- Nutzung privater Endgeräte und externer Speichermedien im Schulnetz,
- angemessene technische Sicherheitsvorkehrungen zur Absicherung des Schulnetzes, der schulischen Endgeräte und des Internetübergangs (wie etwa Firewall-Regeln, Webfilter, ggf. Protokollierung).

In Abstimmung mit dem Schulaufwandsträger können die Aufgabenbereiche vollständig oder teilweise auch auf den Schulaufwandsträger bzw. einen von diesem beauftragten Dienstleister übertragen werden.

Hinsichtlich weiterführender Regelungen wird auf die Bekanntmachung „*Systembetreuung an Schulen“* des Staatsministeriums verwiesen.

3. Verantwortungsbereich des Betreuers oder der Betreuerin des Internetauftritts der Schule

Der Betreuer des Internetauftritts der Schule hat in Abstimmung mit der Schulleitung und gegebenenfalls weiteren Vertretern der Schulgemeinschaft über die Gestaltung und den Inhalt des schulischen Webauftritts zu entscheiden und regelt und überprüft die Umsetzung folgender Aufgaben:

- Auswahl eines geeigneten Webhosters in Abstimmung mit dem Schulaufwandsträger,
- Vergabe von Berechtigungen zur Veröffentlichung auf der schulischen Webseite,
- Überprüfung der datenschutzrechtlichen Vorgaben, insbesondere bei der Veröffentlichung persönlicher Daten und Fotos in Zusammenarbeit mit der bzw. dem örtlichen Datenschutzbeauftragten,
- Regelmäßige Überprüfung der Inhalte des schulischen Internetauftritts,
- Ergreifen von angemessenen sicherheitstechnischen Maßnahmen, um den Webauftritt vor Angriffen Dritter zu schützen, vgl. hierzu die Ausführungen des Bayerischen Landesamts für Datenschutzaufsicht (https://www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf).

Die Gesamtverantwortung für den Internetauftritt der Schule trägt die Schulleitung.

4. Verantwortungsbereich der Lehrkräfte sowie des sonstigen an der Schule tätigen Personals

Die Lehrkräfte sowie sonstiges an der Schule tätiges Personal sind während des Präsenzunterrichts für die Aufsicht über die Schülerinnen und Schüler bei der Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs im Unterricht und zu schulischen Zwecken außerhalb des Unterrichts verantwortlich.

Auch bei der Durchführung von Distanzunterricht hat die Lehrkraft – soweit möglich – auf die Einhaltung der Nutzungsordnung zu achten. Die Aufsichtspflicht während der Teilnahme am Distanzunterricht verbleibt jedoch bei den Erziehungsberechtigten (vgl. § 22 Abs. 3 Satz 3 BaySchO).

5. Verantwortungsbereich der Aufsicht führenden Personen

Die Aufsicht führenden Personen haben auf die Einhaltung der Nutzungsordnungen durch die Schülerinnen und Schüler hinzuwirken.

6. Verantwortungsbereich der Nutzerinnen und Nutzer

Die Nutzerinnen und Nutzer haben die schulische IT-Infrastruktur und den Internetzugang verantwortungsbewusst zu nutzen. Sie sind zu einem sorgsamen Umgang und der Wahrung der im Verkehr erforderlichen Sorgfalt verpflichtet. Sie dürfen bei der Nutzung der schulischen IT-Infrastruktur und des Internetzugangs nicht gegen geltende rechtliche Vorgaben verstoßen.

Nutzerinnen und Nutzer, die unbefugt Software von den schulischen Endgeräten oder aus dem Netz kopieren oder verbotene Inhalte nutzen, können strafrechtlich sowie zivilrechtlich belangt werden. Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung Erziehungs- und Ordnungsmaßnahmen (Schülerinnen und Schüler) bzw. dienst- und arbeitsrechtliche Konsequenzen (Lehrkräfte und sonstiges an der Schule tätiges Personal) zur Folge haben.

B. Besondere Vorschriften für Schülerinnen und Schüler

I. Schutz der schulischen IT-Infrastruktur und des schulischen Internetzugangs

Die Nutzung der schulischen IT-Infrastruktur (Hard- und Software) und des Internetzugangs durch Schülerinnen und Schüler ist an die schulischen Vorgaben gebunden. Dies umfasst insbesondere die Pflicht, schulische Geräte sorgfältig zu behandeln, vor Beschädigungen zu schützen und – sofern erforderlich – für einen sicheren Transport insbesondere mobiler Endgeräte zu sorgen.

Störungen oder Schäden sind unverzüglich der Aufsicht führenden Person bzw. dem Systembetreuer zu melden. Wer schuldhaft Schäden verursacht, hat diese entsprechend den allgemeinen schadensersatzrechtlichen Bestimmungen des BGB zu ersetzen.

II. Nutzung der schulischen IT-Infrastruktur und des schulischen Internetzugangs zu schulischen Zwecken außerhalb des Unterrichts

Die Nutzung der schulischen IT-Infrastruktur und des Internetzugangs zu schulischen Zwecken ist auch außerhalb des Unterrichts gestattet.

C. Besondere Vorschriften für Lehrkräfte und sonstiges an der Schule tätiges Personal

Die Nutzung der schulischen IT-Infrastruktur (Hard- und Software) und des Internetzugangs durch Lehrkräfte oder das sonstige an der Schule tätiges Personal ist an die schulischen Vorgaben

gebunden. Dies umfasst insbesondere die Pflicht, die schulischen Geräte sorgfältig zu behandeln, vor Beschädigungen zu schützen, und – sofern erforderlich – für einen sicheren Transport, insbesondere mobiler Endgeräte, zu sorgen. Jede Nutzerin bzw. jeder Nutzer ist im Rahmen gegebenenfalls bestehender Fortbildungspflichten gehalten, geeignete Fortbildungsangebote wahrzunehmen (vgl. § 9a Abs. 2 Lehrerdienstordnung - LDO).

Für den Umgang mit personalisierten mobilen Endgeräten, die Lehrkräften oder sonstigem an der Schule tätigen Personal zur Erledigung der dienstlichen Aufgaben zur Verfügung gestellt werden, gelten gesonderte Nutzungsbedingungen (siehe Anlage 3 „Nutzungsbedingungen für Lehrerdienstgeräte“).

Störungen oder Schäden sind unverzüglich der Systembetreuung zu melden. Es gelten die Haftungsregeln des jeweiligen Dienst- bzw. Arbeitsverhältnisses, hilfsweise die allgemeinen Haftungsregeln.

D. Schlussvorschriften

Diese Nutzungsordnung tritt am Tag nach ihrer ortsüblichen Bekanntgabe in Kraft. Einmal zu jedem Schuljahresbeginn findet eine Nutzerbelehrung statt, die für Schülerinnen und Schüler, Lehrkräfte und das sonstige an der Schule tätige Personal in geeigneter Weise dokumentiert wird.

Anlagen

- Anlage 1: Erklärung für Lehrkräfte und sonstiges an der Schule tätiges Personal
- Anlage 2: Erklärung für Schülerinnen und Schüler
- Anlage 3: Nutzungsbedingungen für Lehrerdienstgeräte
- Anlage 4: Mindeststandards beim Einsatz dienstlicher Geräte
- Anlage 5: Hinweise zur dienstlichen Nutzung von privaten Endgeräten
- Anlage 6: Mindeststandards beim Einsatz von privaten Endgeräten
- Anlage 7: Nutzungsvereinbarung zum Pilotversuch „Digitale Schule der Zukunft“
- Anlage 8: Nutzung von Microsoft Teams for Education an der Schule
- Anlage 9: Informationen zur Datenverarbeitung nach Art. 13 DSGVO
- KMBek „Hinweise zur Nutzung der IT-Infrastruktur und des Internetzugangs an Schulen“ und „Vollzug des Datenschutzrechts an staatlichen Schulen“ vom 14. Juli 2022

Anlage 1 – Erklärung für Lehrkräfte und sonstiges an der Schule tätiges Personal

Am _____wurde ich _____ in die Nutzungsordnung der Schönwerth-Realschule Amberg (Stand 01.01.2023) zur Nutzung der schulischen IT-Infrastruktur und des Internetzugangs an Schulen eingewiesen. Die in der Nutzungsordnung festgelegten Regelungen habe ich zur Kenntnis genommen.

Mir ist bekannt, dass ich bei einem Verstoß gegen die Nutzungsordnung gegebenenfalls das Recht verliere, die schulische IT-Infrastruktur und den Internetzugang zu privaten Zwecken zu nutzen, und ich gegebenenfalls mit dienst- und arbeitsrechtlichen Konsequenzen rechnen muss.

Zudem ist mir bekannt, dass der Verstoß gegen einschlägige rechtliche Bestimmungen zivil- oder strafrechtliche Folgen nach sich ziehen kann.

Der vollständige Text der Nutzungsordnung ist einsehbar unter
https://www.srsamberg.de/eltern-portal

Bei der Nutzung von Microsoft 365, des schulischen WLANs sowie der schuleigenen iPads werden automatisch personenbezogene Daten verarbeitet. Dies geht nur, wenn hierfür eine Einwilligung vorliegt.

Hierzu möchten wir im Folgenden Ihre Einwilligungen einholen. Die Zugangsdaten werden nach Erteilen der Einwilligungen mitgeteilt.

Hiermit willige ich in die Nutzungsbedingungen von Office 365, des schulisches WLAN sowie der schuleigenen iPads ein, wie zuvor beschrieben:

Bitte ankreuzen!

☐ja/ ☐nein Nutzungsbedingungen von Office 365

☐ja/ ☐nein Nutzungsbedingungen des schuleigenen WLAN

☐ja/ ☐nein Nutzungsbedingungen der schuleigenen iPads

_____

Name der Lehrkraft/des sonstigen an der Schule tätigen Personals

_____

Ort und Datum Unterschrift der Lehrkraft/des sonstigen an der Schule tätigen Personals

Anlage 2 – Erklärung für Schülerinnen und Schüler

Am _____wurde ich in die Nutzungsordnung der Schönwerth-Realschule Amberg (Stand 01.01.2023 zur Nutzung der schulischen IT-Infrastruktur und des Internetzugangs an Schulen eingewiesen. Die in der Nutzungsordnung festgelegten Regelungen habe ich zur Kenntnis genommen.

Mir ist bekannt, dass ich bei einem Verstoß gegen die Nutzungsordnung gegebenenfalls das Recht verliere, die schulische IT-Infrastruktur und den Internetzugang zu privaten Zwecken zu nutzen, und ich gegebenenfalls mit Erziehungs- und Ordnungsmaßnahmen rechnen muss.

Zudem ist mir bekannt, dass der Verstoß gegen einschlägige rechtliche Bestimmungen zivil- oder strafrechtliche Folgen nach sich ziehen kann.

Der vollständige Text der Nutzungsordnung ist einsehbar unter
https://www.srsamberg.de/eltern-portal

_____

Name und Klasse/Jahrgangsstufe

_____

Ort und Datum Unterschrift der Schülerin/des Schülers
(für Schülerinnen und Schüler ab Vollendung des 14. Lebensjahres)

_____

Ort und Datum Unterschrift der/des Erziehungsberechtigten
(bei minderjährigen Schülerinnen und Schülern)

Anlage 3 - Nutzungsbedingungen für Lehrerdienstgeräte

Definition

Lehrerdienstgeräte sind Endgeräte (überwiegend mobile Endgeräte), die dauerhaft oder über einen längeren Zeitraum einer bestimmten Lehrkraft zur dienstlichen Nutzung sowohl innerhalb der Schule als auch außerhalb überlassen werden. Lehrerdienstgeräte verbleiben dabei stets im Eigentum des Schulaufwandsträgers. Die Geräte werden den Nutzern im Rahmen des Beschäftigungsverhältnisses zur Verfügung gestellt.

Zweck der Nutzung

Die Endgeräte werden sowohl für unterrichtliche Zwecke wie die Durchführung, Vor- und Nachbereitung des Unterrichts verwendet, als auch für Verwaltungsaufgaben wie die Eingabe von Zeugnisbemerkungen und Noten, die Erstellung und Verarbeitung von Beurteilungen und den dienstlichen Schriftverkehr.

Die Endgeräte werden in geringem Maße für private Zwecke genutzt (z. B. Schreiben einer Mail, Webseitenaufruf). Die Ablage von privaten Daten ist in geringem Umfang erlaubt. Die private Nutzung darf die Funktionsfähigkeit der Geräte nicht beeinträchtigen.

Verantwortlichkeit für die Funktionsfähigkeit und Sicherheit der Geräte

Die Geräte werden in einem funktionsfähigen Zustand mit installierter Standardsoftware an die Lehrkraft übergeben. Der Lizenznehmer ist bei Beschaffung von Standardsoftware der Sachaufwandsträger.

Veränderungen an der Hardware (z.B. andere Festplatte einbauen) und Veränderungen, die zu einer Beeinträchtigung der Funktionsfähigkeit oder der Sicherheit (Verhinderung von Updates) führen können, sind nicht erlaubt.

Die Lehrkraft verfügt über ein Benutzerkonto und über ein lokales Administrationskonto. Das Administrationskonto darf nur für folgende Zwecke benutzt werden:

- Durchführung von Änderungen an den Einstellungen oder
- Installation von ergänzender Software. Dabei ist zu beachten, dass die erworbene Softwarelizenz den dienstlichen Einsatz zulässt. Die erwerbende Lehrkraft ist der Lizenznehmer und trägt ggf. die notwendigen Kosten. Die Lehrkraft hat den Softwareeinsatz bei der Schulleitung anzuzeigen, damit die Schule ihrer Rechenschaftspflicht nach Art. 5 i.V.m. Art. 32 DSGVO nachgekommen kann. Die Schulleitung kann im Rahmen ihrer organisatorischen Befugnisse eine geeignete Person (z.B. Systembetreuung) mit der Entgegennahme der Anzeige beauftragen.

Hierbei sind die entsprechenden Mindestsicherheitsstandards unter Ziffer 2 umzusetzen.

Bei den vor Schuljahresbeginn 2022/23 ausgegebenen Dienstgeräten ist die Lehrkraft verpflichtet, neben dem bestehenden Administratorkonto ein zusätzliches Benutzerkonto mit Standardrechten einzurichten.

Die Verantwortung für die rechtliche Zulässigkeit der verarbeiteten Daten, einer ergänzenden Softwareinstallation und für die technische Funktionsfähigkeit des Endgeräts nach einem administrativen Eingriff liegt bei der Lehrkraft. Ebenso wird kein Support für zusätzlich installierte Software und der Beeinflussung des generischen Systems durch diese oder bei Änderungen an den Einstellungen geleistet.

Umgang beim Auftreten eines Defektes

Sobald ein Defekt auftritt, ist das Gerät dem Sachaufwandsträger über die Schule zur Überprüfung zu überlassen. Eine vorherige Sicherung der eigenen Daten ist notwendig, da bei der Wiederherstellung möglicherweise die Daten verloren gehen können. Eine eigenmächtige Durchführung oder Veranlassung einer Reparatur ist nicht zulässig.

Rückgabe der Geräte

Lehrerdienstgeräte verbleiben im Eigentum des Schulaufwandsträgers. Die Rückgabe (z.B. Lehrkraft verlässt Schule, neues Gerät wird übergeben, Systemupdate, Garantiefall, Defekt) erfolgt nach Anfrage innerhalb eines angemessenen Zeitraums von maximal zwei Wochen. Nach der Rückgabe der Geräte werden diese in einen Ursprungszustand versetzt (Rücksetzung). Um einen Datenverlust zu vermeiden, ist eine vorherige Sicherung der eigenen Daten auf einem externen Medium notwendig. Vor der Rückgabe müssen die Daten sicher gelöscht werden, um die Einsichtnahme von Unberechtigten zu verhindern.

Mindestsicherheitsstandards beim Einsatz der dienstlichen Geräte

Beim Einsatz der dienstlichen Geräte hat die Nutzerin bzw. der Nutzer die Mindestsicherheits-standards zu beachten (siehe Anlage 4 „Mindestsicherheitsstandards beim Einsatz der dienstlichen Geräte“).

Weitere Informationen

Fortbildungsoffensive für das Unterrichten in einer digitalisierten Welt

- Kurs „Technisches Grundverständnis“: https://fortbildungsoffensive.alp.dillingen.de/

Broschüren

- Sicherheit durch Passwörter: https://schulnetz.alp.dillingen.de/materialien/Passwoerter.pdf
- Datensicherheit durch Verschlüsselung: https://schulnetz.alp.dillingen.de/materialien/Verschluesselung.pdf
- Backup in der Cloud: https://schulnetz.alp.dillingen.de/materialien/Handreichung_Cloud-Backup.pdf

Selbstlernkurse

- Datensicherheit durch Verschlüsselung: https://alp.dillingen.de/lehrgangs-suche/?event_id=285645
- Sicherheit durch Passwörter: https://alp.dillingen.de/lehrgangs-suche/?event_id=285492

Erklärung - Lehrerdienstgeräte

Frau/Herr _____ verpflichtet sich die Nutzungsbedingungen einzuhalten. Verstöße sind Pflichtverletzungen und können dienstrechtlich, arbeitsrechtlich bzw. disziplinarrechtlich geahndet werden und Haftungstatbestände auslösen.

_____

Ort, Datum

_____

Unterschrift der Lehrkraft

Anlage 4 - Mindestsicherheitsstandards beim Einsatz von dienstlichen Geräten

Beim Einsatz der dienstlichen Geräte sind die nachfolgend aufgeführten Mindestsicherheitsstandards zu beachten, um sicherzustellen, dass

- dienstliche Daten vertraulich behandelt werden und
- dienstliche Daten besonders geschützt sind

1. Nutzung eines sicheren Endgeräts und eines sicheren Betriebssystems

Voraussetzung für ein sicheres Endgerät ist, dass das Endgerät von einem vertrauenswürdigen Hersteller stammt und dass alle Tätigkeiten vom Vertrieb bis zur Einrichtung des Endgeräts von vertrauenswürdigen Personen oder Institutionen durchgeführt wurden.

Sicherheitsfunktionen sind heute üblicherweise im Betriebssystem integriert. Dies können restriktive Berechtigungen sein, eigene Schutzprogramme, aber auch App-Stores, die nur das Installieren geprüfter Software ermöglichen. Software sollte nur von anerkannt sicheren Quellen bezogen werden. Unter Windows sind in den Standardeinstellungen eine Firewall und ein Virenscanner aktiv, unter Android können die Berechtigungen der einzelnen Programme auf die Ressourcen eingestellt werden und ein iPad lässt nur die Installation aus dem eigenen App-Store zu.

Werden diese Sicherheitseinstellungen beachtet und die Betriebssysteme sowie Programme regelmäßig (automatisch) aktualisiert, ist ein guter Grundschutz gegeben. Aktuelle Betriebssysteme, die vom jeweiligen Anbieter gepflegt werden, können als sicher betrachtet werden, solange die Sicherheitseinstellungen (vgl. BSI) beachtet bzw. nicht bewusst deaktiviert werden.

2. Sichere Softwareauswahl/-einsatz

2.1 Software aus anerkannt sicheren Quellen

Beim Download und bei der Installation von Software ist generell Vorsicht geboten, da dieser Weg die einfachste Methode darstellt, um Schadsoftware oder unerwünschte Software (z.B. Adware) auf einem Endgerät zu bringen.

Sichere Anbieter von Software sind insbesondere

- Softwareportale der Betriebssysteme (Apple Appstore, Google Playstore, Microsoft Store)
- Webseiten des Herstellers der Hard- oder Software
- vertrauenswürdige Softwareportale, z. B. Heise oder Snapfiles.

Bei vielen Softwareportalen wird allerdings oft zusätzlich Adware mitinstalliert.

2.2 Installation der Software

Die Software ist nur mit dem geringsten notwendigen Funktionsumfang zu installieren und auszuführen.

2.3 Software zur Verarbeitung personenbezogener Daten

Vor dem Erwerb der Software, durch die personenbezogene Daten verarbeitet werden, hat eine Freigabe durch die Schulleitung zu erfolgen.

3. Betrieb des Endgeräts in einer sicheren Netzwerkumgebung

In einem schulischen Netzwerk (z. B. Lehrernetz) mit Zugangsbeschränkungen, kann davon ausgegangen werden, dass das Netzwerk sicher ist und dass aus dem Netzwerk heraus keine Angriffe auf einem Endgerät erfolgen. Entsprechendes gilt auch für das Heimnetzwerk, wenn man ein sicheres WLAN-Passwort gesetzt und am Heimrouter keine Verbindungen von außen ins Heimnetz geöffnet hat. Einschränkungen gelten gegebenenfalls, wenn schlecht abgesicherte Smart-Home-Geräte im Heimnetz betrieben werden, die von sich aus einer Internetverbindung öffnen.

Betrieb des Endgeräts in unterschiedlichen Umgebungen

Wenn dienstliche Endgeräte in unterschiedlichen Umgebungen genutzt werden, fehlt der Schutz der schulischen oder häuslichen Umgebung und des lokalen Netzwerks. Deshalb muss in besonderer Weise sichergestellt sein, dass

- das Endgerät vor unberechtigten physischen Zugriffen geschützt ist und
- das Endgerät vor Angriffen bzw. unberechtigten Zugriffen aus dem lokalen Netzwerk und aus

dem Internet geschützt ist.

Hier ist in besonderer Weise auf sichere Einstellungen am Endgerät zu achten (Updates, Firewall, Virenscanner, keine Freigaben nach außen) sowie auf eine verschlüsselte Verbindung ins Internet.

4. Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft

Der Zugriff auf das Endgerät darf nur durch die jeweilige Lehrkraft erfolgen. Ist die Nutzerin bzw. der Nutzer an einem Endgerät mit persönlichen Zugangsdaten angemeldet (z. B. mit Benutzernamen und starkem Passwort), ist der Zugriff von fremden Personen zumindest erschwert. Beim Verlassen des Arbeitsplatzes sollte sich die Lehrkraft abmelden oder das Endgerät sperren. Bei zu langer Inaktivität kann auch eine automatische Sperrung des Endgeräts erfolgen.

Wie strikt diese Maßnahmen durchgeführt werden sollten, ist auch von der jeweiligen Umgebung abhängig. Wenn der Zugangsschutz zum persönlichen Endgerät durch andere Maßnahmen erfolgt (z. B. in einem ausschließlich selbst genutzten Büro) können auch einfachere Schutzmaßnahmen am Endgerät genügen.

5. Verschlüsselte Ablage von dienstlichen Daten

Die verschlüsselte Ablage von Dateien oder Dokumenten bietet auch dann noch Schutz, wenn diese in die falschen Hände geraten. Bei der Verschlüsselung von Daten steht die Vertraulichkeit im Vordergrund. Es soll gewährleistet sein, dass ohne den zugehörigen Schlüssel bzw. ohne das Passwort die Dokumente nicht lesbar sind. Der zugehörige Schlüssel muss an einem sicheren Ort aufbewahrt werden.

Möglich ist die Verschlüsselung einzelner Dokumente, die Ablage der Dokumente in verschlüsselten Containern oder die Verschlüsselung ganzer Partitionen bzw. Dateisysteme.

6. Speicherfristen

Die gesetzlichen Aufbewahrungsfristen sind einzuhalten.

7. Backup der dienstlichen Daten

Sofern ein Backup erstellt wird, muss auf den Zugriffsschutz und auf eine Verschlüsselung geachtet werden. Um einem Verlust der Daten vorzubeugen, empfiehlt es sich, regelmäßig Sicherungskopien der wichtigen Daten anzufertigen und diese an einem sicheren Ort aufzubewahren. Bei Backups sind ebenfalls die unter Ziffer 6 genannten Aufbewahrungsfristen einzuhalten.

8. Sicheres Löschen von Datenträgern

Bei ausgemusterten Geräten müssen die Datenträger vor der Entsorgung oder Weitergabe an Dritte sicher gelöscht oder vernichtet werden.

9. Gerätespezifische Voreinstellungen /-installationen

Bei den ausgegebenen Convertibles wurden zur Grundverschlüsselung Bitlocker eingeschaltet sowie die Programme Keepass (Passwortverwaltung), Cryptomator (Daten-Verschlüsselung) und Eraser (sicheres Löschen) installiert.

Anlage 5 – Hinweise zur dienstlichen Nutzung von privaten Endgeräten

Definition

Private Endgeräte stehen weder im Eigentum des Schulaufwandsträgers, noch werden sie von der Schule zentral verwaltet.

Subsidiarität und inhaltliche Grenzen der Verarbeitung personenbezogener Daten

Personenbezogene Daten dürfen mit privaten Endgeräten nur verarbeitet werden, soweit kein schulisches Endgerät zur Verfügung steht.

Endgeräte in der häuslichen Umgebung

Wenn private Endgeräte, auf denen vertrauliche dienstliche Daten gespeichert oder verarbeitet werden, ausschließlich zu Hause genutzt werden (z. B. bei Desktop-Endgeräten), ist mindestens sicherzustellen, dass dienstliche Daten vertraulich behandelt werden und dienstliche Daten besonders geschützt sind.

Die technischen Möglichkeiten, wie diese Bedingungen erreicht werden können, sind:

- Nutzung eines sicheren Endgerätes und eines sicheren Betriebssystems
- Betrieb des Endgerätes in einer sicheren Netzwerkumgebung
- Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft
- Verschlüsselte Ablage von vertraulichen dienstlichen Daten
- Backup der dienstlichen Daten
- Sicheres Löschen von Daten

Endgeräte in unterschiedlichen Umgebungen

Wenn private Endgeräte, auf denen vertrauliche dienstliche Daten gespeichert oder verarbeitet werden, in unterschiedlichen Umgebungen genutzt werden (z.B. mobile Endgeräte), fehlt gegebenenfalls der Schutz der häuslichen Umgebung und des lokalen Netzwerks. Deshalb muss zusätzlich zu den obigen Bedingungen in besonderer Weise sichergestellt sein, dass das Endgerät vor unberechtigten physischen Zugriffen geschützt ist und vor Angriffen bzw. unberechtigten Zugriffen aus dem lokalen Netzwerk und aus dem Internet geschützt ist.

Private Endgeräte in schulischen Umgebungen

Wenn private Endgeräte in schulischen Umgebungen genutzt werden (z. B. im WLAN der Schule), darf von diesen Endgeräten keine Gefahr oder Beeinträchtigung für das schulische Netzwerk oder für die anderen Endgeräte in dem schulischen Netzwerk ausgehen. Deshalb ist darauf zu achten, dass das Endgerät keine Software enthält, die in der Lage wäre, das Netzwerk in der Schule auszuspionieren oder andere Endgeräte anzugreifen (z. B. Schadsoftware), und sich die Nutzung des Internetzugangs der Schule im üblichen Rahmen bewegt.

Weitere Informationen: Fortbildungsoffensive für das Unterrichten in einer digitalisierten Welt

Kurs „Technisches Grundverständnis": https://fortbildungsoffensive.alp.dillingen.de/

Anlage 6 - Mindestsicherheitsstandards beim Einsatz von privaten Endgeräten

Beim Einsatz von privaten Endgeräten zur dienstlichen Aufgabenerfüllung hat die Nutzerin bzw. der Nutzer die Mindestsicherheitsstandards zu beachten.

1. Nutzung eines sicheren Endgerätes und eines sicheren Betriebssystems

Voraussetzung für ein sicheres Endgerät ist, dass das Endgerät von einem vertrauenswürdigen Hersteller stammt und dass alle Tätigkeiten vom Vertrieb bis zur Einrichtung des Endgerätes von vertrauenswürdigen Personen oder Institutionen durchgeführt wurde.

Sicherheitsfunktionen sind heute üblicherweise im Betriebssystem integriert. Dies können restriktive Berechtigungen sein, eigene Schutzprogramme, aber auch App-Stores, die nur das Installieren geprüfter Software ermöglichen. Software sollte nur von anerkannt sicheren Quellen bezogen werden.

- Unter Windows sind in den Standardeinstellungen eine Firewall und ein Virenscanner (Microsoft Defender) aktiv.
- Bei Apple MacOS ist die Firewall und der Virenscanner integriert und aktiv.
- Unter Android können die Berechtigungen der einzelnen Programme auf die Ressourcen eingestellt werden, ein iPad lässt nur die Installation aus dem eigenen App-Store zu.
- Bei Tablets ist der Schutz in der Systemsicherheit integriert.

Werden diese Sicherheitseinstellungen beachtet und die Betriebssysteme sowie Programme regelmäßig (automatisch) aktualisiert, ist ein guter Grundschutz gegeben.

Aktuelle Betriebssysteme, die vom jeweiligen Anbieter gepflegt werden, können als sicher betrachtet werden, solange die Sicherheitseinstellungen beachtet bzw. nicht bewusst deaktiviert werden.

2. Software aus anerkannt sicheren Quellen

Beim Download und bei der Installation von Software ist generell Vorsicht geboten, da dieser Weg die einfachste Methode darstellt, um Schadsoftware oder unerwünschte Software (z. B. Adware) auf einem Endgerät zu bringen.

Sichere Anbieter von Software sind insbesondere

- Softwareportale der Betriebssysteme (Apple Appstore, Google Playstore, Microsoft Store)
- Webseiten des Herstellers der Hard- oder Software
- vertrauenswürdige Softwareportale, z. B. Heise oder Snapfiles.
  Bei vielen Softwareportalen wird allerdings oft zusätzlich Adware mitinstalliert.

3. Betrieb des Endgerätes in einer sicheren Netzwerkumgebung

Hat man ein sicheres WLAN-Passwort gesetzt und am Heimrouter keine Verbindungen von außen ins Heimnetz geöffnet, kann man davon ausgehen, dass das Heimnetz sicher ist. Einschränkungen gelten gegebenenfalls, wenn schlecht abgesicherte Smart-Home-Geräte im Heimnetz betrieben werden, die von sich aus einer Internetverbindung öffnen.

Im Allgemeinen kann man davon ausgehen, dass ein lokales Netz zu Hause sicher ist, solange kein Zugriff von außen möglich ist und innerhalb des Heimnetzes nur sichere Geräte betrieben werden.

4. Internetverbindungen in einer unsicheren Umgebung

In potenziell unsicheren Netzwerkumgebungen (z. B. in einem öffentlichen WLAN) muss man auf Internetverbindungen nicht grundsätzlich verzichten. Voraussetzung ist, dass man an einem sicheren Endgerät (z. B. eigenes Notebook oder eigenes Tablet) arbeitet, das nicht manipuliert wurde, dass man in besonderer Weise auf sichere Einstellungen an seinem Endgerät achtet (Updates, Firewall, Virenscanner, keine Freigaben nach außen) sowie auf eine verschlüsselte Verbindung ins Internet – sobald persönliche oder vertrauliche Daten übertragen werden.

5. Zugriff auf das Endgerät nur durch die jeweilige Lehrkraft

Wenn man an einem Endgerät mit persönlichen Zugangsdaten angemeldet ist (z. B. mit Benutzername und Passwort) ist der Zugriff von fremden Personen zumindest erschwert. Beim Verlassen des Arbeitsplatzes sollte man sich abmelden oder das Endgerät sperren. Bei zu langer Inaktivität sollte eine automatische Sperrung des Endgerätes erfolgen.

<u>Weitere Informationen:</u>

Broschüre: https://schulnetz.alp.dillingen.de/materialien/Passwoerter.pdf ;

Selbstlernkurs: https://alp.dillingen.de/lehrgangs-suche/?event_id=285492

Wie strikt diese Maßnahmen durchgeführt werden sollten, ist auch von der jeweiligen häuslichen Umgebung abhängig. Wenn der Zugangsschutz zum persönlichen Endgerät durch andere Maßnahmen erfolgt (z. B. in einem ausschließlich selbst genutzten Arbeitszimmer) können auch einfachere Schutzmaßnahmen am Endgerät genügen.

6. Ablage von dienstlichen Daten

Die dienstlichen Daten sollten logisch und organisatorisch von den privaten Daten und den Systemdaten getrennt sein (z. B. in unterschiedlichen Verzeichnissen). Die verschlüsselte Ablage von Dateien oder Dokumenten bietet auch dann noch Schutz, wenn diese in die falschen Hände geraten. Bei der Verschlüsselung von Daten steht die Vertraulichkeit im Vordergrund. Es soll gewährleistet sein, dass ohne den zugehörigen Schlüssel bzw. ohne das Passwort die Dokumente nicht lesbar sind.

Möglich sind die Verschlüsselung einzelner Dokumente, die Ablage der Dokumente in verschlüsselten Containern oder die Verschlüsselung ganzer Partitionen bzw. Dateisysteme (Festplattenverschlüsselung). Bei mobilen Endgeräten sollte die Festplatte verschlüsselt werden.

<u>Weitere Informationen:</u>

Datensicherheit durch Verschlüsselung:
https://schulnetz.alp.dillingen.de/materialien/Verschluesselung.pdf

Selbstlernkurs: Datensicherheit durch Verschlüsselung: https://alp.dillingen.de/lehrgangs-suche/?event_id=285645

7. Löschfristen

Die gesetzlichen Aufbewahrungsfristen sind einzuhalten.

8. Backup der dienstlichen Daten

Um einem Verlust der Daten vorzubeugen, empfiehlt es sich, regelmäßig Sicherungskopien der wichtigen Daten anzufertigen und diese an einem sicheren Ort aufzubewahren. Auch bei einem Backup muss auf den Zugriffsschutz und ggf. auf eine Verschlüsselung geachtet werden. Die unter Ziffer 7 genannten Löschfristen sind einzuhalten.

Sofern das Backup in der Cloud außerhalb des EWR/EU-Raums erfolgt, ist darauf zu achten, dass die personenbeziehbaren Daten Dritter nicht ohne weitere Sicherheitsmaßnahmen (z.B. angemessene und geeignete Verschlüsselung) abgelegt werden.

Weitere Informationen:

Backup in der Cloud: https://schulnetz.alp.dillingen.de/materialien/Handreichung_Cloud-Backup.pdf

9. Entsorgung des Endgerätes

Vor der Entsorgung oder Weitergabe des Endgerätes ist dafür zu sorgen, dass die dienstlichen Daten zuverlässig gelöscht sind.

Anlage 7 – iPad-Nutzungsvereinbarung zum Pilotversuch „Digitale Schule der Zukunft“

Mit dem Tablet hast du ein großartiges technisches Hilfsmittel für einen modernen, multimedialen Unterricht in der Hand. Damit du gewinnbringend damit arbeiten kannst und während der Nutzung keine Probleme auftauchen, haben wir für dich Tablet-Nutzung Regeln aufgestellt, die dir in der Schule dabei helfen sollen, möglichst gut mit dem neuen Medium zu lernen.

Diese Regelung ist für die erfolgreiche Nutzung eines Tablets als ein Hilfsmittel für den Unterricht unerlässlich. Die Verwendung des Geräts ist nur unter Einhaltung dieser Nutzungsordnung zulässig.

Grundsätzlich:

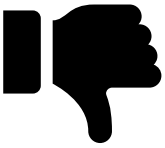
- Jede Schülerin und jeder Schüler geht sorgsam mit dem Tablet um.
- Während der Pausen ist die Verwendung des iPads ausschließlich zur Vorbereitung auf den Unterricht an geeigneten Orten gestattet.
- Die Handynutzung bleibt weiterhin untersagt.
- Das iPad darf ansonsten nur benutzt werden, wenn die Lehrkraft dazu auffordert.
- In der Schule dient das Tablet als **Lernwerkzeug**, nicht zur Unterhaltung.
- Das iPad, der Eingabestift sowie die Kopfhörer werden immer mit in die Schule gebracht.
- Das iPad (und Zubehör) soll zuhause immer vollständig aufgeladen werden.
- Ich achte darauf, ausreichend Speicherkapazität für die schulische Arbeit freizuhalten.
- Ich versende keine **illegalen** Bilder oder Videos (verfassungsfeindlich, pornographisch, rassistisch, gewalttätig usw.).
- Auf meinem Tablet sind keine **illegalen** Bilder oder Videos gespeichert, hier beachte ich auch das **Urheber- und Persönlichkeitsrecht.**
- Ich habe alle benötigten Apps installiert.
- Die Installation von großen Apps und Updates führe ich zuhause durch, um das WLAN der Schule nicht zu überlasten.
- Die Daten auf dem iPad sind stets durch ein Backup zu sichern. Das regelmäßige Anfertigen von Sicherungskopien erstellter Arbeitsmaterialien liegt überdies in der Verantwortung der Schülerinnen und Schüler.

In der Schule / im Unterricht

- Mitschriften auf dem Tablet erfolgen durch einen aktiven digitalen Stift in dem jeweils pro Fach angelegten Team in einem OneNote-Klassennotizbuch. Die Lehrkraft kann in Ausnahmefällen auch die Tastatur zulassen.

- Mit der App „Classroom“ kann die Lehrkraft im Unterricht Einblick in den aktuell bearbeiteten Bildschirm aller Schülerinnen und Schüler erhalten und bei Bedarf einzelne Apps oder auch das iPad sperren. Zu weiteren gespeicherten Daten hat die Lehrkraft allerdings keine Zugangsberechtigung. Außerhalb des Klassenzimmers ist der Zugriff auf die iPads nicht mehr möglich. Eine Nutzung der App “Classroom” wird akzeptiert. Die MDM Verwaltungssoftware JAMF gestattet es den Lehrkräften Einschränkungen im gleichen Funktionsumfang wie bei der „Classroom“ App durchzuführen, jedoch ist eine Anzeige des Bildschirms nicht möglich. Die Privatsphäre der Schülerinnen und Schüler bleibt hierdurch gewahrt.
- Jede zweckfremde Nutzung des Tablets während des Unterrichts (z. B. Dateien oder Nachrichten an Mitschülerinnen oder Mitschüler senden, Spiele spielen usw.) ist ausdrücklich verboten und wird mit entsprechenden Maßnahmen geahndet.
- Unerlaubte Audio-, Bild- oder Videomitschnitte aus einer Unterrichtsstunde sind strengstens untersagt und ziehen entsprechende schul- und zivilrechtliche Konsequenzen nach sich.
- Der unerlaubte Zugriff auf Präsentationsmedien (z. B. Clevertouch Board) ist nicht erlaubt. Der Zugriff darf nur nach Aufforderung durch die Lehrkraft erfolgen.
- Wenn ich das Tablet während des Unterrichts nicht brauche, liegt es **zugeklappt** auf dem Tisch. In Phasen der Nichtnutzung soll das Gerät in den Flugmodus versetzt oder der Bildschirm abgedunkelt werden.
- Während des Unterrichts surfe ich nur zu den angegebenen Websites.
- Es ist den Schülerinnen und Schülern während des Unterrichts nicht erlaubt im Internet zu surfen oder Dateien aus diesem zu laden, außer nach Aufforderung durch die Lehrkraft.
- Ich mache keine Fotos, Tonaufnahmen und Videos von Mitschülern oder Lehrkräften, außer sie stimmen diesen ausdrücklich zu.
- Auf den Tablets anderer Schülerinnen und Schüler darf ohne deren Wissen und Zustimmung nichts gelöscht, verändert oder installiert werden.
- Im Unterricht verschicke ich **ungefragt** keine Nachrichten.

Verhaltensregeln Tablet

 Ich achte darauf, dass das Tablet immer aufgeladen ist.	 Ich achte darauf, dass auf dem Tablet genügend freier Speicherplatz vorhanden ist.	 Mitschriften erfolgen mit digitalem Stift. Nur in genehmigten Ausnahmefällen nutze ich die Tastatur.
 Ich benutze das iPad im Unterricht nur, wenn mich meine Lehrkraft dazu auffordert.	 Ich benutze nur Apps und Programme, die ich für eine Aufgabe verwenden soll.	 Eine zweckfremde Nutzung des Tablets während des Unterrichts ist untersagt.
 Ein unerlaubter Zugriff auf Präsentationsmedien (Clevertouch, Apple TV) ist nicht gestattet.	Digitale Schule der Zukunft	 Ich nehme keine unerlaubten Änderungen an Hard- und Software vor.
 Ich beachte stets das Urheberrecht und den Datenschutz.	 Film-, Bild- und Tonaufnahmen sind ohne ausdrückliche Erlaubnis einer Lehrkraft (Betroffener) unzulässig.	 Wenn ich im Unterricht ein Video oder Musik anschaue / anhöre, verwende ich dazu Kopfhörer.
 Ich werde niemanden über das iPad bedrohen, beleidigen oder verletzen.	 Nicht jugendfreie Inhalte darf ich weder laden noch speichern.	 Ich sorge dafür, dass mein Gerät außerhalb des Unterrichts sorgfältig und sicher verwahrt ist.

Erklärung - iPad-Nutzung

Die Schüler übernimmt keinerlei Haftung für Diebstahl oder Schäden am Gerät bzw. Zubehör. Der jeweilige Lernende ist für alles, was auf und mit dem Gerät geschieht, verantwortlich und hat dafür zu sorgen, dass keine missbräuchliche Fremdnutzung erfolgen kann.

Für überlassene Leihgeräte tragen die Schülerinnen und Schüler während der Nutzung die Verantwortung. Eigenmächtige Veränderungen an Hard- und Software sind nicht zulässig. Störungen oder Schäden sind sofort zu melden.

Mir ist bewusst, dass Verstöße gegen diese Punkte zum Nutzungsverbot des Tablets führen sowie Erziehungs- und Disziplinarmaßnahmen (z. B. Verweis) und in groben Fällen auch rechtliche Schritte nach sich ziehen können.

_____

Name und Klasse/Jahrgangsstufe

_____

Ort und Datum Unterschrift der Schülerin/des Schülers
(für Schülerinnen und Schüler ab Vollendung des 14. Lebensjahres)

_____

Ort und Datum Unterschrift der/des Erziehungsberechtigten
(bei minderjährigen Schülerinnen und Schülern)

Anlage 8 – Nutzung von Microsoft 365 inklusive Teams for Education an der Schule

1. Anwendungsbereich

Diese Nutzungsbedingungen regeln die Nutzung des von der Schule bereitgestellten digitalen Office- bzw. Kommunikationswerkzeugs Microsoft 365 inkl. Teams for Education.

Sie gelten für alle Schülerinnen und Schüler, die Teams nutzen, und gehen insoweit den bestehenden EDV-Nutzungsbedingungen der Schule vor.

2. Zulässige Nutzung

Die Nutzung der Plattform ist nur für schulische Zwecke zulässig. Sie dient dazu, die schulischen Kommunikations- und Lernangebote zu unterstützen bzw. sinnvoll zu ergänzen.

3. Anlegen von Konten für Schülerinnen und Schüler

Die Nutzung von Microsoft 365 ist für Schülerinnen und Schüler freiwillig. Nutzerkonten für Schülerinnen und Schüler werden nur angelegt, wenn sie (bzw. bei Minderjährigen deren Erziehungsberechtigte) den Nutzungsbedingungen für Schülerinnen und Schüler zugestimmt und ihr Einverständnis mit der damit verbundenen Datenverarbeitung erklärt haben. Bei Schülerinnen und Schülern zwischen 14 und 18 Jahren ist zusätzlich deren Zustimmung erforderlich.

4. Nutzung mit privaten Geräten

Die Nutzung von Microsoft 365 ist grundsätzlich über den Internetbrowser des Nutzer-Geräts möglich. Die Installation der verschiedenen Microsoft-Apps ist nicht notwendig und erfolgt ggf. in eigener Verantwortung der Nutzerinnen und Nutzer.
Beim Einsatz mobiler (privater) Geräte müssen diese mindestens durch eine PIN oder ein Passwort geschützt werden.

5. Datenschutz und Datensicherheit in Bezug auf Teams for Education

Das Gebot der Datenminimierung ist zu beachten: Bei der Nutzung sollen so wenig personenbezogene Daten wie möglich verarbeitet werden. Insbesondere das Entstehen nicht benötigter Schülerdaten beim Einsatz von Teams ist vermeiden.

Die Aufzeichnung einer Bild-, Ton- oder Videoübertragung, z. B. durch eine Software oder das Abfotografieren des Bildschirms, ist nicht gestattet.

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.

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.

Die Zugangsdaten dürfen nicht an andere Personen weitergegeben werden. Wer vermutet, dass sein Passwort anderen Personen bekannt geworden ist, ist verpflichtet, dieses zu ändern. Die Verwendung eines fremden Nutzerkontos ist grundsätzlich unzulässig.

Nach Beendigung der Nutzung haben sich die Nutzerinnen und Nutzer bei Teams auszuloggen.

Eine Verwendung des schulischen Nutzerkontos zur Authentifizierung an anderen Online-Diensten ist nicht zulässig, außer es ist ein von der Schule zugelassener Dienst.

6. Verbotene Nutzungen

Die Schülerinnen und Schüler sind verpflichtet, bei der Nutzung der Plattform geltendes Recht einzuhalten, u. a. das Strafrecht und das Jungendschutzrecht. Außerdem ist jede Nutzung untersagt, die geeignet ist, die berechtigen Interessen der Schule zu beeinträchtigen (z. B. Schädigung des öffentlichen Ansehens der Schule; Schädigung der Sicherheit der IT-Ausstattung der Schule).

Es ist verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Plattform abzurufen, zu speichern oder zu verbreiten. Von den Teilnehmerinnen und Teilnehmern über Teams bereitgestellte Inhalte dürfen nicht unbefugt in sozialen Netzwerken verbreitet werden.

7. Verstoß gegen die Nutzungsbedingungen

Im Falle eines Verstoßes gegen diese Nutzungsbedingungen behält sich die Schulleitung das Recht vor, den Zugang zu Microsoft 365 zu sperren. Davon unberührt behält sich die Schulleitung weitere Maßnahmen vor.

8. Schlussbestimmungen

Nach dem Ende der Bereitstellung des Angebots werden alle Daten inklusive der Nutzer-Accounts nach einer Übergangszeit gelöscht.

Tritt eine Schülerin oder ein Schüler während der Vertragslaufzeit aus einer angemeldeten Schule aus (beispielsweise durch Schulwechsel) und wird daher vom Schul-Admin das Nutzerkonto dieser Person entfernt, wird dieses nach 30 Tagen unwiderruflich gelöscht. Daneben gibt es die Möglichkeit, Nutzerkonten direkt zu löschen.

Anlage 9 – Informationen zur Datenverarbeitung nach Art. 13 DSGVO

Name und Kontaktdaten des Verantwortlichen

Für die Datenverarbeitung ist die jeweilige Schule verantwortlich, deren Kontaktdaten sie auch im Briefkopf bzw. der Fußzeile finden:

Schönwerth-Realschule
Fuggerstr. 15
92224 Amberg

09621 91565-0
09621 91565-105
sekretariat@schoenwerth-realschule.de

Kontaktdaten des Datenschutzbeauftragten

Wir möchten Sie auf die Kontaktdaten des Datenschutzbeauftragten der Schule hinweisen, die Sie auch in den Datenschutzhinweisen unserer Schulhomepage finden können:

Markus Braun
- persönlich -
Fuggerstr. 15
92224 Amberg

09621 91565-0
markus.braun@schoenwerth-realschule.de

Zwecke und Rechtsgrundlagen für die Verarbeitung Ihrer Daten

Die Schule verarbeitet die personenbezogenen Daten im Rahmen von Microsft 365 für schulische Zwecke. Rechtsgrundlage für die Verarbeitung der Daten ist eine Einwilligung der betroffenen Personen.

Empfänger von personenbezogenen Daten

Schulinterne Empfänger (Schulleitung und von der Schulleitung beauftragte Schul-Admins mit Benutzerwaltungsrechten, Lehrkräfte sowie Schülerinnen und Schüler der eigenen Lerngruppe(n)) nach den konkret zugewiesenen Berechtigungen innerhalb der Schule.

Zur Bereitstellung und Nutzung von Microsoft 365 ist die Übermittlung personenbezogener Daten an ausgewählte Dienstleister notwendig. Mit diesen Dienstleistern hat die Schule eine Vereinbarung zur Datenverarbeitung im Auftrag der Schule geschlossen (sog. „Auftragsverarbeitung“ nach Art. 28 DSGVO). Die Schule bedient sich folgender Auftragsverarbeiter:

Microsoft Ireland Operations, Ltd. One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521. Die Verarbeitung erfolgt zur Bereitstellung des Cloud Service „Microsft 0ffice365“ einschließlich der zugehörigen Wartungs-, Pflege- und Supportleistungen; Microsoft speichert die folgenden „ruhenden“ Daten auf Servern nur innerhalb der Europäischen Union:

(1) E-Mail-Postfachinhalte (E-Mail-Text, Kalendereinträge und Inhalt von E-Mail-Anhängen),

(2) SharePoint Online-Websiteinhalte und die auf dieser Website gespeicherten Dateien sowie

(3) Dateien, die auf den Cloudspeicher OneDrive for Business hochgeladen wurden.

Nähere Informationen zu Teams und den datenschutzrechtlichen Angaben finden Sie unter https://privacy.microsoft.com/de-de/privacystatement.

Folgende Datenarten sind Gegenstand der Verarbeitung:
Anzeigename, Familienname, Vorname, Externe ID, Klasse, Kurse, Kursjahr bzw. Schuljahr, E-Mailadresse, Technische Protokolldaten, Benutzername, Personenrolle, Person, Benutzergruppe, Benutzerzugang (aktiv, gesperrt), Sprache, E-Mailadresse, Letzte Anmeldung, Office 365 Tenant ID, Profileinstellungen, Passwort (verschlüsselt)/Anmeldename;

Zusätzlich bei Lehrkräften / nicht-unterrichtenden Personal:
unterrichtete Fächer/Kurse, unterrichtete Klassen, Gruppenzugehörigkeit (z. B. Fachschaft), Protokollierung der Nutzung (kurzfristige Aufbewahrung)

Im Übrigen können Kundendaten und personenbezogenen Daten, die Microsoft im Auftrag der Schule verarbeitet, auf der Basis der EU-Standardvertragsklauseln auch in Länder außerhalb der Europäischen Union („Drittstaaten“, z. B. USA) übermittelt werden, um die Onlinedienste bereitzustellen.

Dauer der Speicherung der personenbezogenen Daten

Tritt eine Person während der Vertragslaufzeit aus einer angemeldeten Schule aus (beispielsweise durch Wegzug) und wird daher vom Schul-Admin das Nutzerkonto dieser Person entfernt, wird dieses nach 30 Tagen unwiderruflich gelöscht. Daneben gibt es die Möglichkeit, Personen direkt zu löschen. Mit Ende der zentral koordinierten Bereitstellung des Angebotswerden alle Daten inklusive der Nutzer-Accounts nach einer Übergangszeit gelöscht.

Weitere Informationen

Für nähere Informationen zur Verarbeitung Ihrer Daten können Sie sich an den Verantwortlichen sowie Datenschutzbeauftragten der Schule wenden (s. o.). Eine Übersicht an Informationen zum Datenschutz im Zusammenhang mit dem Einsatz von Teams finden Sie außerdem unter https://km.bayern.de/teams-datenschutz im Bereich „Weitere Informationen zum Datenschutz beim Einsatz von Teams“.

Datenverarbeitung – Erklärung für Lehrkräfte und sonstiges an der Schule tätiges Personal

Ich stimme hiermit den Nutzungsbedingungen zur Nutzung von Microsoft 365 inklusive Teams for Education zu. Weiterhin willige ich ein, dass die Schule ein entsprechendes Nutzerkonto anlegt und die oben aufgeführten Daten in diesem Zusammenhang an Microsoft übermittelt und von diesen verarbeitet werden.

Hiermit willige ich in die Verarbeitung von personenbezogenen Daten der oben bezeichneten Person bei der Nutzung von Microsoft 365 durch die Schule und Microsoft ein. Die Informationen zur Datenverarbeitung habe ich zur Kenntnis genommen.

Diese Einwilligung in die Datenverarbeitung kann jederzeit bei der Schule widerrufen werden. Durch den Widerruf wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung, nicht berührt.

Die Einwilligung ist freiwillig. Bei Nichterteilung oder dem Widerruf der Einwilligung kann das Angebot von Microsoft 365 nicht genutzt werden.

_____

Name der Lehrkraft/des sonstigen an der Schule tätigen Personals

_____

Ort und Datum, Unterschrift der Lehrkraft/des sonstigen an der Schule tätigen Personals

Datenverarbeitung – Erklärung Schüler

Ich stimme hiermit den Nutzungsbedingungen zur Nutzung von Microsoft 365 inklusive Teams for Education zu. Weiterhin willige ich ein, dass die Schule ein entsprechendes Nutzerkonto anlegt und die oben aufgeführten Daten in diesem Zusammenhang an Microsoft übermittelt und von diesen verarbeitet werden.

Hiermit willige ich in die Verarbeitung von personenbezogenen Daten der oben bezeichneten Person bei der Nutzung von Microsoft 365 durch die Schule und Microsoft ein. Die Informationen zur Datenverarbeitung habe ich zur Kenntnis genommen.

Diese Einwilligung in die Datenverarbeitung kann jederzeit bei der Schule widerrufen werden. Durch den Widerruf wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung, nicht berührt.

Die Einwilligung ist freiwillig. Bei Nichterteilung oder dem Widerruf der Einwilligung kann das Angebot von Microsoft 365 nicht genutzt werden.

_____

Name und Klasse/Jahrgangsstufe

_____

Ort und Datum Unterschrift der Schülerin/des Schülers
(für Schülerinnen und Schüler ab Vollendung des 14. Lebensjahres)

_____

Ort und Datum Unterschrift der/des Erziehungsberechtigten
(bei minderjährigen Schülerinnen und Schülern)