

Nutzungsordnung zur Nutzung der IT-Infrastruktur und des Internetzugangs an der Markgrafenschule

A. Allgemeiner Teil

I. Allgemeines und Geltungsbereich

Die Markgrafenschule 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 Systembetreuer der Markgrafenschule (systembetreuer@mgs-bt.de) 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 der Systembetreuerin oder des Systembetreuers durchgeführt werden oder wenn temporäre Veränderungen im Rahmen des Unterrichts explizit vorgesehen sind.

Private Endgeräte und externe Speichermedien dürfen nur mit Zustimmung des Systembetreuers, 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

Zur Nutzung der von der Schule zur Verfügung gestellten IT-Infrastruktur und Dienste (z. B. Zugriff auf persönliches Netzlaufwerk) ist eine individuelle 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 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).

Alle erzeugten Daten werden nach Abschluss der Analysen unwiderruflich gelöscht.

Durch die Nutzung von LogoDIDACT und aSc EduPage werden zudem auch Anmeldedaten und persönliche Daten (Name, Vorname, Geburtsdatum bei Schülern und Schülerinnen) protokolliert oder gespeichert.

Erhobene Daten, im Rahmen der Nutzung von LogoDIDACT:

Login/Logout-Zeitpunkt; Daten beim Speichern von Dateien (Name des Eigentümers); personenbezogene Daten in LOG-Dateien, z.B. Webseitenaufrufe.

Genauere Informationen sind der Verfahrensbeschreibung oder den technischen Details von LogoDIDACT zu entnehmen (einsehbar im Sekretariat der Markgrafenschule).

Erhobene Daten, im Rahmen der Nutzung von aSc EduPage:

Login/Logout Zeitpunkt; Grunddaten der Lehrkräfte (Name, Vorname, Namenskürzel, E-Mailadresse, unterrichtete Fächer, Abwesenheit, Sprechstunden); Grunddaten der Schüler (Name, Vorname, Geburtsdatum, Klassenzugehörigkeit, Abwesenheit); Daten der Eltern (Name, Vorname, E-Mailadresse)

Genauere Informationen sind der Verfahrensbeschreibung oder den technischen Details von aSc EduPage zu entnehmen (einsehbar im Sekretariat der Markgrafenschule).

6. Speicherplatz innerhalb der schulischen IT-Infrastruktur

Beim Zugriff auf den Nutzerinnen und Nutzern von der Schule zur Verfügung gestellten persönlichen Speicherplatz innerhalb der schulischen IT-Infrastruktur ist eine Authentifizierung notwendig.

Die Schule fertigt von diesem persönlichen Verzeichnis Sicherheitskopien (Backup) an.

Die Schule bietet zudem eine schul-, klassen- oder kursspezifische Austauschverzeichnisstruktur unter folgender Adresse <https://nextcloud.mgs.logoip.de> an, auf dem jede Schülerin und jeder Schüler sowie jede Lehrkraft oder sonstiges an der Schule tätiges Personal mit persönlicher Authentifizierung Dateien bereitstellen kann. Dieses Austauschverzeichnis dient dem schnellen Dateiaustausch während des Unterrichts.

7. Private Nutzung der schulischen IT-Infrastruktur

Schülerinnen und Schülern ist es gestattet, den Internetzugang (WLAN) außerhalb des Unterrichts und anderen Lernzeiten 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.

Die Nutzungsordnung gewährt Lehrkräften ein Recht zur Nutzung der IT-Infrastruktur und des Internets zu privaten Zwecken. Die Lehrkräfte versichern durch ihre Unterschrift, dass sie die Nutzungsordnung anerkennen. Die vorherige Einwilligung der Lehrkraft ist Voraussetzung für die Nutzung der IT-Infrastruktur und des Internets zu privaten Zwecken. Die Lehrkraft kann die Einwilligung jederzeit widerrufen. Im Fall des Widerrufs ist die Nutzung der IT-Infrastruktur und des Internets zu privaten Zwecken nicht mehr gestattet.

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

8. 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.

9. 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.

10. 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.

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 Netzwerkkumgebung
- 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.

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 Markgrafenschule 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 Markgrafenschule 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

Die Anmeldung am WLAN erfolgt über Service Set Identifier (SSID)

MGS Hotspot. Die Nutzerin bzw. der Nutzer bestätigen vor dem Surfen die Nutzungsvereinbarungen der Telekom. Es sind keine weiteren Benutzerdaten erforderlich. Die Nutzungsvereinbarungen müssen jeden Tag neu bestätigt werden.

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.

Die Schule stellt bei der Nutzung des schulischen Internetzugangs über private Endgeräte keine zentralen Sicherheitsinstanzen (z. B. Virenschutz o. ä.) zur Verfügung.

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 alleine 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 Bezirk Oberfranken als 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

Die Systembetreuerin bzw. der Systembetreuer berät die Schulleitung zusammen mit der bzw. dem Datenschutzbeauftragten bei der konkreten Gestaltung und Nutzung der schulischen IT-Infrastruktur und des Internetzugangs sowie der Abstimmung mit dem zuständigen Schulaufwandsträger. Die Systembetreuerin bzw. 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 oder die Betreuerin 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.lida.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 sorgsamem 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 oder dem Systembetreuer zu melden. Wer schuldhaft Schäden verursacht, hat diese entsprechend den allgemeinen Schadensersatzrechtlichen Bestimmungen des BGB zu ersetzen. Bei Schülerinnen und Schülern, die das 18. Lebensjahr noch nicht vollendet haben, hängt die deliktische Verantwortlichkeit von der für die Erkenntnis der Verantwortlichkeit erforderlichen Einsicht ab (§ 823 Abs. 3 Bürgerliches Gesetzbuch - BGB). Elektronische Geräte sind durch Schmutz und Flüssigkeiten besonders gefährdet; deshalb sind während der Nutzung der Schulcomputer Essen und Trinken verboten.

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 tätige 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.

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.