

Nutzungsordnung für die Nutzung digitaler Endgeräte am Gymnasium bei St. Stephan, Augsburg

*Die Nutzungsordnung gilt für alle Schülerinnen und Schüler,
alle Lehrkräfte und sonstiges an der Schule tätiges Personal verbindlich.*

A. Allgemeiner Teil

I. Allgemeines und Geltungsbereich

Das Gymnasium bei St. Stephan 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.

II. Regeln für jede Nutzung

II.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 oder Systembetreuer gemeldet werden. Dies betrifft insbesondere öffentlich gewordene Passwörter oder falsche Zugangsberechtigungen.

II.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. Externe Speichermedien dürfen nur mit Zustimmung einer Lehrkraft oder einer Aufsicht führenden Person an die schulische IT-Infrastruktur oder das Schulnetz angeschlossen werden.

II.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 er-

forderlich. Nach Beendigung der Nutzung haben sich die Nutzerinnen und Nutzer abzumelden. An den Schülergeräten der Computerräume und Bibliotheken kann der Bildschirminhalt vom Lehrer zur Wahrung der Aufsichtspflicht eingesehen werden.

II.4 Anmeldung im Verwaltungsnetz

Im Verwaltungsnetz werden besonders schützenswerte Daten verarbeitet. Daher ist eine benutzer-spezifische Authentifizierung notwendig. Die Berechtigungen werden nach Maßgabe von Aufgaben und Erfüllung schulischer Zwecke verteilt.

II.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.

Siehe dazu auch II.3 und Anhang A.

II.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 – konkret die persönlichen Verzeichnisse auf den PCs in der Schule – ist eine Authentifizierung notwendig. Die Schule fertigt von diesem persönlichen Verzeichnis keine Sicherheitskopien (Backup) an.

Schützenswerte (z. B. personenbezogene) Daten müssen hinreichend vor Fremdzugriff geschützt werden (z. B. Passwortschutz). Die Inhalte dieses Verzeichnisses werden in unregelmäßigen Abständen z. B. beim Zurücksetzen der PCs gelöscht.

II.7 Private Nutzung der schulischen IT-Infrastruktur

Schülerinnen und Schülern ab der Jahrgangsstufe 8 sowie den Lehrkräften und sonstigem an der Schule tätigen Personal ist es gestattet, mobile Endgeräte außerhalb des Unterrichts und anderer Lernzeiten in geringem Umfang zu privaten Zwecken zu nutzen, entsprechend der *Regelungen zur Nutzung digitaler Medien am Gymnasium bei St. Stephan*. 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.

II.8 Verbotene Nutzungen

Die rechtlichen Bestimmungen – insbesondere des Strafrechts, des Urheberrechts, des Datenschutzrechts und des Jugendschutzrechts – sind zu beachten. Es ist insbesondere verboten, pornographische, sexistische, 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.

II.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 zur Verfügung gestellten Hinweise, abrufbar unter:

<http://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.

II.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, wenn sie den *Regelungen zur Nutzung digitaler Medien am Gymnasium bei St. Stephan* entsprechend erfolgen und die technischen Anforderungen an das Endgeräte erfüllt werden.

Technische Anforderungen an das Endgerät:

- a. Das Gerät muss den geltenden Normen und Vorgaben der verwendeten Vernetzungstechnik entsprechen. Es dürfen keine Störungen der IT-Infrastruktur der Schule und des Internetzugangs von diesem Gerät verursacht werden.
- b. Die Software des Gerätes, Betriebssystem sowie installierte Apps, müssen auf dem aktuellen Stand sein. Insbesondere müssen alle sicherheitsrelevanten Updates eingespielt sein. Die Installation von Updates sollte möglichst automatisiert erfolgen.
- c. Auf dem Gerät muss, soweit dies das Betriebssystem erfordert, ein aktueller Virens Scanner installiert sein, der selbständig seine Datenbank aktualisiert.

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.

III.1 Gestattung zur Nutzung des kabellosen Internetzugangs (WLAN)

Das Gymnasium bei St. Stephan, Augsburg, 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. Das Gymnasium bei St. Stephan, Augsburg, 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.

III.2 Zugang zum schulischen WLAN

Zugang zum schulischen WLAN über einen gemeinsamen Schlüssel (Pre-Shared-Key): Die Schule stellt der Nutzerin bzw. dem Nutzer für die Mitbenutzung des Internetzugangs Zugangsdaten über einen gemeinsamen Schlüssel (Pre-Shared-Key) zur Verfügung (Zugangssicherung). Die Nutzerinnen und Nutzer haben dabei denselben Zugangsschlüssel, der in gewissen Abständen geändert und über einen Aushang in den Klassenzimmern/per E-Mail

bekannt gegeben wird. Diese Zugangsdaten dürfen nicht an Dritte weitergegeben werden. Die Schule kann diese Zugangsdaten jederzeit ändern bzw. in ihrer Gültigkeit zeitlich beschränken.

III.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 Stadt Augsburg 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.

III.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, 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.

III.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.

III.6 Protokollierung

Bei der Nutzung des schulischen Internetzugangs wird aus technischen Gründen die MAC-Adresse des benutzten Endgeräts erfasst und diesem eine hausinterne IP-Adresse zugeordnet.

Es findet keine allgemeine Protokollierung der Aktivitäten der Nutzerin bzw. des Nutzers statt. Es ist der Systembetreuung in Absprache mit der Schulleitung dennoch aus begründetem Anlass erlaubt, vorübergehend eine Protokollierung zu technischen Zwecken durchzuführen, z. B. zur Erkennung von Bandbreitenengpässen.

Siehe dazu auch Anhang A.

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:

IV.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.

IV.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.

IV. 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.

IV.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).

IV.5 Verantwortungsbereich der Aufsicht führenden Personen

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

IV.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

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 zu melden. Wer schuldhaft Schäden verursacht, hat diese entsprechend den allgemeinen schadensersatzrechtlichen Bestimmungen des BGB zu ersetzen.

Klassenchats, auch auf nicht-schulischen Plattformen wie WhatsApp u. ä., sind zwar grundsätzlich als private Kommunikationswege einzustufen. Da sie jedoch Auswirkungen auf das schulische Miteinander haben können, behält sich die Schulleitung bei missbräuchlichem Verhalten die Einleitung pädagogischer Maßnahmen oder schulrechtlicher Konsequenzen vor. Bei strafrechtlich relevanten Sachverhalten ist die Schulleitung zur Einschaltung der Polizei verpflichtet.

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.

Anhang A

Regelung des Schulaufwandsträger zum Datenschutz

1. Die Stadt Augsburg erhebt personenbeziehbare Daten betroffener Personen entspr. Art. 13 und Art. 14 DSGVO.
2. Verantwortlich für die Datenerhebung ist die Stadt Augsburg, Rathausplatz 1, 86150 Augsburg, augs-burg@augzburg.de, Telefon +49 821 324-0. Ein verschlüsseltes Kontaktformular (<https://www.augszburg.de/kontakt/>) finden Sie auf unserer Homepage.
3. Kontaktdaten des Datenschutzbeauftragten: Stadtverwaltung Augsburg, Datenschutzbeauftragte/r, Hermanstraße 1, 86150 Augsburg, datenschutz@augzburg.de, Telefon +49 821 324-2666
4. Die Daten werden auf Grundlage von Art. 6 Abs. 1 Buchstabe a bzw. c verarbeitet.
5. Die Daten werden auf WLAN-Access Points, WLAN-Management-Systemen, Switches, Routern und Firewalls erfasst, die zwangsläufig für die Bereitstellung des Internetzugangs benutzt werden müssen.
6. Das Amt für Digitalisierung, Organisation und Informationstechnik der Stadt Augsburg ist berechtigt folgende Daten zusammen mit einem Zeitstempel für bis zu 1 Jahr zu speichern sowie für die Analyse von Fehlern oder Missbrauch und die Erkennung von Trends mit anderen Daten zu verknüpfen:
 - a. MAC- und IP-Adressen, Betriebssystem, Hostname der angeschlossenen Geräte,
 - b. wesentliche Protokollinformationen für die Datenübertragung im Internet auf Schicht 3 und 4 wie die verwendeten TCP- und UDP-Ports,
 - c. angeforderte DHCP-Optionen,
 - d. Dauer und Datenvolumen der Nutzung,
 - e. bei unverschlüsseltem HTTP die aufgerufene URL und den User-Agent-Header des Browsers,
 - f. bei WLAN: Signalstärke und Geolokation des Gerätes,
7. Beim Zugang über WLAN werden diese Daten außerdem für den Betrieb und die Überwachung der WLAN-Infrastruktur durch die Firma Hewlett Packard Enterprise für bis zu 90 Tage in einem Amazon Web Services Rechenzentrum in Frankfurt am Main gespeichert und verarbeitet. Weitere Informationen über die Datenverarbeitung können unter <https://www.arubanetworks.com/dataprivacy/> im Datenblatt für Aruba Central nachgelesen werden.
8. Nach der Datenschutz-Grundverordnung stehen Ihnen folgende Rechte zu. Da nur Daten erfasst werden, die nur über die Verknüpfung von Zeitraum, MAC-Adresse und Nutzungsort einen Rückschluss auf ein Gerät, aber nicht direkt auf eine Person erlauben, ist es für die Ausübung der folgenden Rechte erforderlich, dass Sie den Zeitraum, die MAC-Adresse des verwendeten Gerätes und den Ort der Nutzung nennen:
 - a. Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht, Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO). Bitte beachten Sie, dass dieses Auskunftsrecht in bestimmten Fällen eingeschränkt oder ausgeschlossen sein kann (vgl. insbesondere Art. 10 BayDSG).
 - b. Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Art. 16 DSGVO).
 - c. Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen (Art. 17 und 18 DSGVO).
 - d. Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO).
 - e. Aus Gründen, die sich aus Ihrer besonderen Situation ergeben, können Sie die Verarbeitung Sie betreffender personenbezogener Daten durch uns zudem jederzeit widersprechen (Art. 21 DSGVO). Sofern die gesetzlichen Voraussetzungen vorliegen, verarbeiten wir in der Folge diese Daten nicht mehr.
 - f. Sollten Sie von Ihren oben genannten Rechten Gebrauch machen, prüft die öffentliche Stelle, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind.
 - g. Weiterhin besteht ein Beschwerderecht beim Bayerischen Landesbeauftragten für den Datenschutz (<https://www.datenschutz-bayern.de/service/>).
9. Wenn Sie in die Verarbeitung durch die Stadt Augsburg durch die Nutzung des Zugangs eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen (Art. 13 Abs. 2 Buchst. c DSGVO). Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.