Inhalt

Nutzungsordnung des pädagogischen IT-Netzes der Holstenschule.....2

Nutzungsordnung für das Lernmanagementsystem (LMS) „itslearning“.....5

Hinweise zur Datenverarbeitung im Rahmen der Nutzung des LMS „itslearning“.....9

Nutzungsordnung für den KI-Chatbot „telli“.....12

Informationen über die Verarbeitung Ihrer Daten beim telli-Chatbot.....13

Präambel

Diese Ordnung enthält die allgemeinen Regeln für die Nutzung des pädagogischen IT-Netzwerks der Holstenschule. Sie soll sicherstellen, dass geltendes Recht eingehalten wird und das pädagogische IT-Netz intakt bleibt. Die schulische Computereinrichtung soll den Schüler*innen für die Nutzung im Rahmen des Unterrichts, der Projektgruppenarbeit und zur Festigung der Medienkompetenz innerhalb und außerhalb des Unterrichts zur Verfügung stehen. Dafür ist ein sorgfältiger und verantwortungsbewusster Umgang mit den Geräten und Einrichtungen eine wichtige Voraussetzung.

Begriffsklärungen

Nutzer*innen sind Schülerinnen und Schüler, Lehrkräfte sowie Mitarbeiterinnen und Mitarbeiter der Schule, die sich verpflichtet haben, diese Ordnung einzuhalten und daraufhin Zugang zum pädagogischen IT-Netzwerk der Schule erhalten haben.

Das **pädagogische IT-Netzwerk** der Schule umfasst alle schuleigenen stationären und mobilen Geräte sowie Installationen, die im Zusammenhang mit Unterricht zur Produktion, Speicherung und Übermittlung digitaler Inhalte in der Schule vorgehalten werden, und damit auch die Anwendungen des Schulportals Neumünster. Es enthält die Bereiche LAN und WLAN.

Private Endgeräte, denen Zugang zum pädagogischen IT-Netzwerk gewährt wird, werden für die Zeit des Zugangs zu Teilen des pädagogischen IT-Netzwerks und unterliegen diesem Regelwerk.

Nutzung umfasst alle Verfahren der Datenproduktion, der Datenspeicherung und Datenübertragung, soweit dazu das pädagogische IT-Netzwerk verwendet wird.

Filterung, Protokollierung, Datenschutz

Die Schule und der Schulträger sind verantwortlich für die Einhaltung der datenschutzrechtlichen Vorgaben und zur Wahrnehmung ihrer Aufsichtspflicht berechtigt, den Datenverkehr gemäß § 11 (4) SchulDSVO zu protokollieren und zu kontrollieren. Hierbei werden personenbezogene Nutzungsdaten temporär gespeichert. Diese können im Fall einer missbräuchlichen Nutzung des Zugangs personenbezogen an Strafverfolgungsbehörden übermittelt werden.

Die Wahrung des Fernmeldegeheimnisses im Sinne des § 88 TKG wird gewährleistet. Die für die Computerinfrastruktur Verantwortlichen halten die ihnen im Zusammenhang mit ihrer Tätigkeit für die vorgenannten Systeme bekannt gewordenen Daten geheim.

Verpflichtungen der Nutzer*innen

Die Nutzer*innen sind verpflichtet, die geltenden gesetzlichen Bestimmungen, die Bestimmungen des Strafrechts, des Jugendschutzrechts und des Urheberrechts einzuhalten.

Es ist untersagt,

- das IT-Netz und seine Teile für private Zwecke zu verwenden,
- das IT-Netz und seine Teile zu beschädigen oder zu zerstören,
- die Struktur des IT-Netzes durch die Installation fremder Hard- und Software zu verändern,
- persönliche Daten Dritter (z.B. Name, Geburtsdatum, Personenfotos/-videos) unberechtigt im Internet zu veröffentlichen,
- Dateien (z.B. Musikstücke und Filme) aus File-Sharing-Netzwerken herunterzuladen,
- Kopierschutz- und Filtermechanismen zu umgehen,
- Inhalte, die dem Ansehen oder dem Erscheinungsbild der Schule oder an der Schule tätigen Personen schaden, zu verbreiten sowie
- illegale, pornografische, gewaltverherrlichende, rassistische oder jugendgefährdende Inhalte aufzurufen, zu erstellen, zu bearbeiten, zu speichern oder zu veröffentlichen.

Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen.

Bei der Weiterverarbeitung von Daten aus dem Internet sind die Urheber- und Nutzungsrechte zu beachten.

Aus hygienischen Gründen ist das Trinken und Essen bei der Nutzung schulischer Endgeräte nicht erlaubt, da die Tastaturen durch Schmutz und Flüssigkeiten besonders gefährdet sind.

Meldung von Störungen und Schäden
Die Nutzer*innen sind verpflichtet, Störungen oder Schäden am pädagogischen IT-Netz unverzüglich der zuständigen Lehrkraft bzw. der Schulleitung zu melden.

Missbrauch, Manipulation, mutwillige Beschädigung
Wenn Nutzer*innen das pädagogische IT-Netz missbräuchlich verwenden, beschädigen oder (auch versuchsweise) manipulieren, wird das jeweilige Nutzungskonto gesperrt und es werden Ordnungsmaßnahmen nach § 25 SchulG verhängt. Die Nutzer*innen kommen für selbst verursachte Schäden auf. Rechtlich relevante Tatbestände werden durch die Holstenschule zur Anzeige gebracht. Sollten Nutzer*innen Kenntnis erlangt haben, dass rechtswidrige Inhalte im pädagogischen Netz gespeichert werden, müssen sie die zuständige Lehrkraft unverzüglich darüber informieren.

Datensicherheit
Bei der Nutzung privater Geräte übernimmt die Holstenschule keine Haftung für die Datensicherheit dieser Geräte. Die Verantwortung hierfür liegt ausschließlich bei den Nutzer*innen.

Vertragsverhältnisse gegenüber Dritten
Schülerinnen und Schüler dürfen im Internet weder im Namen der Holstenschule noch im Namen anderer Personen Verträge abschließen. Ohne Erlaubnis der Schulleitung dürfen für die Holstenschule keine kostenpflichtigen Dienste im Internet in Anspruch genommen werden.
Die Veröffentlichung von Inhalten im Namen oder unter dem Namen der Holstenschule bedarf stets der Genehmigung durch die Schulleitung oder einer durch sie autorisierten Person. Dies gilt auch im Falle von Veröffentlichungen außerhalb der Schul-Homepage – etwa im Rahmen von Schul- oder Unterrichtsprojekten.

Weitere technische Bestimmungen
Da die Bandbreite des schulischen Internetzugangs limitiert ist, müssen – soweit dies möglich ist – die automatischen Update-Funktionen auf privaten Endgeräten abgestellt sein. Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien aus dem Internet ist zu vermeiden. Sollten Nutzer*innen außerhalb schulischer Zwecke oder sonst unberechtigt Daten im IT-Netzwerk oder auf schulischen Geräten ablegen, ist die Schulleitung bzw. die für die Computernutzung zuständige Person berechtigt, diese Daten zu löschen.

Lernmanagementsystem (LMS) itsLearning und Lernplattform Moodle
Der Zugang zum LMS itsLearning und zur Lernplattform Moodle erfolgt grundsätzlich personenbezogen in Kombination von Benutzername und zugehörigem Passwort. Nach Beendigung der Nutzung meldet sich der Nutzer von der Lernplattform ab. Die Zugangsdaten dürfen nicht weitergegeben werden. Im Zweifelsfall haftet der/die registrierte Nutzer*in für unzulässige Aktivitäten Dritter. Sollte ein/e Nutzer/in sein/ihr Passwort vergessen haben, kann er/sie persönlich bei den Administratoren ein neues beantragen.

Ein Anspruch darauf, Nutzer*in zu werden, besteht nicht. Ein Missbrauch kann den Verlust des Nutzer*innenstatus zur Folge haben. Die Schule kann die Nutzungsmöglichkeiten beschränken.
Für die LMS und die Lernplattform gelten die einschlägigen datenschutzrechtlichen Regelungen.

Über die in der Anmeldung angegebenen, teils automatisch anfallenden, teils vom Nutzer zusätzlich eingegebenen Informationen hinaus protokolliert die der Lernplattform zugrunde liegende Software in einer Datenbank, zu welcher Zeit welche Nutzer*innen auf welche Bestandteile der Lehrangebote bzw. Profile anderer Nutzer*innen zugreifen. Protokolliert wird unter anderem, ob Teilnehmer*innen gestellte Aufgaben erledigen, ob und welche Beiträge sie in den eventuell angebotenen Foren leisten, ob und wie sie in Workshops mitwirken. Diese Daten sind nur den Administratoren der Lernplattform und der Leitung der jeweiligen Lehrveranstaltung zugänglich, nicht jedoch (von Daten im Zusammenhang mit Aufgaben, Workshops und Foren abgesehen) anderen Nutzern*innen. Sie dienen ausschließlich der Durchführung der jeweiligen Lehrveranstaltung und werden nicht an andere Personen oder Stellen weitergegeben, auch nicht in anonymisierter Form. Die Administration der Lernplattform sowie die Leitung der jeweiligen Lehrveranstaltung versichert, dass die Protokolle statistisch nicht ausgewertet werden.

Besondere Regelungen für die Nutzung privater Endgeräte zu unterrichtlichen Zwecken

Private Endgeräte unterliegen während der schulischen Nutzung diesem Regelwerk. Anweisungen der Lehrkräfte bezüglich der Nutzung ist Folge zu leisten. Auf Aufforderung ist Lehrkräften Einblick in die schulische Dokumentation zu gewährleisten.

Die Schule übernimmt keinerlei Haftung für Schäden an privaten Endgeräten oder Diebstahl. Schäden, die durch Dritte entstehen, sind durch private Haftpflichtversicherungen zu regulieren.

Besondere Regelungen für die Nutzung des Schülerarbeitsraumes (Raum 4)

Das Arbeiten an einem Computer in Raum 4 ist für schulische Zwecke für Schüler*innen ab Klasse 7 in Freistunden und Mittagspausen möglich. Vor der erstmaligen Nutzung ist eine Einweisung durch Schüler*innen der Medienscouts-AG erforderlich. Weiterhin gelten die Regeln der „Nutzungsordnung Schülerarbeitsraum“, die in Raum 4 aushängt.

Ende des Nutzungsverhältnisses

Mit dem Austritt der Nutzer*innen aus der Schulgemeinschaft der Holstenschule werden der Zugang und die hinterlegten gespeicherten Daten gelöscht.

Inkrafttreten

Diese Nutzungsordnung tritt am 02. Februar 2026 in Kraft.

Neumünster, den 02. Februar 2026

Der Schulleiter

Nutzungsordnung für das Lernmanagementsystem (LMS) „itslearning“ an der Holstenschule Neumünster

Präambel

Das für Bildung zuständige Ministerium des Landes Schleswig-Holstein stellt den schleswig-holsteinischen Schulen das webbasierte Lernmanagementsystem (LMS) „itslearning“ (https://sh.itslearning.com/) für die pädagogische Arbeit zur Verfügung. Jede Schule erhält eine schuleigene LMS-Instanz. Das System ermöglicht eine datenschutzkonforme Kommunikation und Kooperation zu unterrichtlichen Zwecken. Lehrkräfte haben die Möglichkeit, unter anderem digitale Unterrichtsmaterialien bereitzustellen, auszutauschen und Aufgaben bzw. Aufträge zu erteilen sowie Rückmeldungen zu Arbeitsergebnissen der Schülerinnen und Schüler zu geben. Für die unterrichtliche Nutzung bietet das LMS sowohl eine digitale Austauschplattform als auch digitale und interaktive Werkzeuge, um Unterricht zu gestalten, gemeinsam an Projekten zu arbeiten und miteinander zu kommunizieren. Darüber hinaus existiert eine Integration des Videokonferenzdienstes Big Blue Button (BBB) im LMS.

Zugang zum LMS und Passwortschutz

Der Zugang zum LMS erfolgt über das Schulportal SH. Hierfür wird ein sogenanntes Single-Sign-On (SSO) verwendet, d.h. die Anmeldedaten (Benutzername, Passwort) für das Schulportal SH und das LMS sind identisch. Nutzerinnen und Nutzer können aus dem Schulportal SH heraus über die entsprechende „Kachel“ auf die LMS-Instanz ihrer Schule zugreifen oder aber sie melden sich über https://sh.itslearning.com/ bzw. die itslearning-App direkt an.

Der Zugang zum Schulportal SH und somit zum LMS ist durch ein Passwort geschützt. Die nachfolgenden Bedingungen für ein sicheres Passwort sind zu beachten:

- mindestens 8 Zeichen
- mindestens 1 Ziffer
- mindestens 1 Kleinbuchstabe
- mindestens 1 Großbuchstabe
- mindestens 1 Sonderzeichen
- kein Leerzeichen

Zur Teilnahme an unterrichtlichen Aktivitäten ist seitens der Nutzerinnen und Nutzer sicherzustellen, dass sie mit Benutzernamen und Passwort auf ihre Konten zugreifen und arbeiten können.

Für den Fall, dass das Passwort vergessen wurde, kann dies durch die Schulportal-Administration zurückgesetzt werden. Die Schulportal-Administration ist über folgenden Weg zu erreichen:

Thomas Riefle thomas.riefle@schule-sh.de
Viktoria Mincheva viktoria.mincheva@schule-sh.de

Allgemeine Verhaltensregeln

- Die Nutzung des LMS ist allein für unterrichtliche Zwecke zulässig. Eine Nutzung des Systems zu kommerziellen-, nicht schulbezogenen- oder Schulverwaltungszwecken ist unzulässig. Ausnahme ist die Verarbeitung folgender personenbezogener Daten der Schülerinnen und Schüler: Name, die Zugehörigkeit zu einer bestimmten Klasse oder Lerngruppe, die bei der Nutzung erzeugten Daten der Nutzerinnen und Nutzer sowie technische Nutzdaten (vgl. § 11 Abs. 4 SchulDSVO).
- Die einschlägigen gesetzlichen Bestimmungen (u. a. Datenschutzrecht, Urheberrechtsgesetz, Strafgesetzbuch, Bürgerliches Gesetzbuch, Digitale-Dienste-Gesetz) sind zu beachten und einzuhalten.
- Jede Gefährdung bzw. Beeinträchtigung Dritter ist zu unterlassen.
- Alle Nutzerinnen und Nutzer verpflichten sich, in Foren, Gruppendiskussionen, Chats usw. respektvoll miteinander umzugehen und die Rechte anderer zu wahren.
- Massen-Nachrichten o. ä. sind nicht gestattet.
- Die Weitergabe von Inhalten (inklusive bspw. Screenshots von Chats, Chatverläufe, Video-, oder Audiomitschnitten), die den Nutzerinnen und Nutzern über das LMS zugänglich sind, ist unzulässig.

- Die Nutzerinnen und Nutzer tragen die Verantwortung für die Inhalte und die Art selbstständig erstellter, gespeicherter und versendeter Daten und Dokumente.
- Die Schülerinnen und Schüler werden durch die Klassenlehrkräfte im Rahmen des Unterrichts über die relevanten Vorgaben altersgerecht aufgeklärt.
- Eltern unterstützen ihr Kind ebenfalls bei Verständnis und Einhaltung der gesetzlichen Vorgaben.

Verhaltensregeln bei der Nutzung der Dateiablage

- Um die zentrale, von Ort und Endgerät unabhängige Nutzung des LMS sicherzustellen, sind Daten und Dokumente direkt im LMS zu speichern.
- Die Eingabe und Speicherung von personenbezogenen Daten durch die Schülerin bzw. den Schüler selbst, wie beispielsweise die Nennung des eigenen Namens oder der Namen Dritter in eigenen Dokumenten, sollte nur in dem zur Aufgabenerfüllung erforderlichem Maße und unter Beachtung der Wahrung der Rechte Dritter erfolgen (bspw. in Unterlagen zu Referaten, Aufsätzen usw.).
- Das Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte ist ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten.

Verhaltensregeln bei Hausaufgaben

- Hausaufgaben können in digitaler Form über das LMS gestellt, eingereicht und kommentiert werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum und eine entsprechende Rückmeldung.

Verhaltensregeln bei Videokonferenzen

- Videokonferenzen werden nur durch Lehrkräfte gestartet.
- Nutzerinnen und Nutzer werden beim Betreten eines Videokonferenzraumes ggf. aufgefordert, sich einen Namen zu geben. Hier sind Vor- und Nachname anzugeben.
- Lehrkräfte haben das Recht und die Pflicht bei unbekannten Teilnehmerinnen und Teilnehmern nachzufragen, wer sich hinter einem Namen verbirgt.
- Nutzerinnen und Nutzer schalten Kamera und Mikrofon nur an, wenn Sie durch die Lehrkraft dazu aufgefordert werden. Die Nutzung der Videofunktion (Kamerabild) ist freiwillig.
- Es besteht das Risiko, durch Benutzung der Videofunktion innerhalb des Wohnumfeldes ungewollt/unbewusst Informationen preiszugeben (z. B. durch Poster an der Wand). Nutzerinnen und Nutzer Sie die "Blur"-Funktion, um den Hintergrund unscharf zu zeichnen.
- Es dürfen keine persönlichen Informationen über die Chat-Funktion oder die geteilten Notizen ausgetauscht werden.
- Chat-Verläufe und geteilte Notizen dürfen nur zur Sicherung von Arbeitsergebnissen und nur in Absprache mit der Lehrkraft exportiert werden.
- Weitere Personen dürfen nur teilnehmen / mit im Raum sein, soweit es für die Durchführung der Konferenz erforderlich ist (z.B. Eltern bei jüngeren Schulkindern)
- Alle Nutzerinnen und Nutzer verlassen nach Beendigung einer Konferenz den Raum. Die jeweilige Lehrkraft verlässt den Raum zuletzt.
- Die jeweilige Lehrkraft schließt nach der Veranstaltung den Videokonferenzraum.

Verstöße

Verwendet eine Schülerin bzw. ein Schüler das System entgegen der Nutzungsordnung oder den Anweisungen der Lehrkraft im Unterricht und wird hierdurch der Lernerfolg beeinträchtigt oder der Unterricht gestört, so können gemäß § 25 SchulG Ordnungsmaßnahmen ausgesprochen werden.

Verstoßen Nutzerinnen und Nutzer gegen diese Nutzungsordnung oder besteht ein begründeter Verdacht auf missbräuchliche Nutzung, ist die Schul-Administration berechtigt, sowohl eigenständig als auch nach

Meldung durch eine Lehrkraft bzw. die Schulleiterin oder des Schulleiters das jeweilige Benutzerkonto kurzfristig und vorübergehend zu sperren (z.B. zur Beweissicherung oder Maßnahme gemäß § 25 SchulG). Ebenso dazu berechtigt ist die sogenannte Site-Administration für das LMS auf Landesebene.

Die Schulleitung ist über Sperrungen umgehend zu informieren.
Über den Zeitpunkt der Aufhebung der Sperre entscheidet die Schulleitung. Betroffene Nutzerinnen und Nutzer sind über das Vorgehen zu informieren.

Verletzungen des Schutzes personenbezogener Daten
Sollte der Verdacht bestehen, dass sich Dritte unbefugt Zugang zu Daten im LMS verschafft haben bzw. einen entsprechenden Versuch unternommen haben, ist umgehend die Schulleitung sowie die Schuladministration zu informieren. Die Schulleitung informiert den zentralen Datenschutzbeauftragten für die öffentlichen Schulen im für Bildung zuständigen Ministerium.

Datenschutz - Löschung - Protokollierung
Die Löschung der nutzungsbezogenen Daten erfolgt grundsätzlich regelmäßig zum Schuljahreswechsel. Ein Benutzerkonto – inklusive aller zugehöriger Daten und Dateien – wird am Ende der Schul- oder Dienstzeit bzw. bei Wegzug aus dem Bundesland Schleswig-Holstein gelöscht. Die Nutzerinnen und Nutzer haben vor der Löschung selbst dafür Sorge zu tragen, eigenständig eingestellte Daten und Dateien aus der persönlichen Dateiablage durch Download für eine mögliche weitere Nutzung zu sichern (Backup).

Log-Dateien (sogenannte Protokolle) werden bei der Arbeit mit dem LMS systemseitig und auf der Grundlage von bestehenden gesetzlichen Regelungen vorübergehend gespeichert. In begründeten Fällen (Missbrauch wie bspw. Mobbing) werden diese Protokolldaten ggf. durch die Schulleitung und mit hierfür bestimmten Personen – wie gesetzlich vorgeschrieben – eingesehen und ausgewertet. Falls es notwendig ist, wird auch die Polizei eingeschaltet.

Ausführliche Informationen zum Datenschutz und Ihren diesbezüglichen Rechten finden Sie im separaten Dokument „Hinweise und Informationen zum Datenschutz“.

Funktionen und Module

Lehrkräfte – Unterrichtsplanung
Die Unterrichtsverteilung ist die Grundlage für die Kurs- und Unterrichtsstruktur. Mit dem Unterrichtsplaner lassen sich Materialien, Themen und Standards verbinden, Pläne dynamisch verändern, mit anderen Lehrkräften sowie Schülerinnen und Schülern teilen. Als weitere Instrumente stehen das Kompetenzraster und zur Verfügung.

Kurse, Aufgaben, Aufträge – Forumsdiskussionen
Zu unterrichtlichen Zwecken legen Lehrkräfte Kurse im LMS an und richten den entsprechenden Kreis von teilnehmenden Schülerinnen und Schülern ein. Aufgaben und Aufträge werden dabei durch die jeweilige Lehrkraft einzelnen Schülerinnen und Schülern oder Gruppen zugewiesen. Diese Möglichkeiten umfassen u.a. interaktive Materialien in Formaten wie Umfrage, Diskussion, Test oder Quiz. Bei Gruppenarbeiten haben Schülerinnen und Schüler die Möglichkeit, auch untereinander bspw. Aufgaben zu stellen, einzureichen und Feedback zu geben. Sogenannte Projekte bieten kollaborative Räume, in denen Schülerinnen und Schüler an gemeinsamen Projekten arbeiten können. In einem E-Portfolio können von Schülerinnen und Schülern oder Lehrkräften Kurs-basierte persönliche Portfolios erstellt werden.

Lernpfade

Für die Lehrkräfte ist es im Rahmen von Binnendifferenzierung möglich, jeder Schülerin und jedem Schüler einen individuellen Weg über die sogenannten „Lernpfade“ anzulegen, um das Erlangen der anzustrebenden Kompetenzen zu befördern.

Bibliothek

Für eine Materialsammlung steht den Lehrkräften das Modul „Bibliothek“ zur Verfügung. Beim Einstellen und Verwenden von Inhalten sind die Hinweise zum „Urheberrecht an Schule“ (https://www.schleswig-holstein.de/DE/Fachinhalte/L/lehrer_innen/urheberrecht.html) unbedingt zu beachten.

Messaging, Benachrichtigungen, Mitteilungen

Das Instant Messaging System im LMS erlaubt eine interne Kommunikation in Echtzeit zu unterrichtlichen und unterrichtsorganisatorischen Zwecken.

Kalender

Über die Kalender-Funktion des LMS erfolgt die Zusammenschau auf alle Kurs-Kalender, einen persönlichen Kalender, Raum- und Ressourcenbuchung sowie alle Unterrichtspläne.

Dateiablage – Speichern von Dateien

Nutzerinnen und Nutzer erhalten eine eigene Dateiablage. Das System erlaubt es jederzeit, die selbst eingestellten Dateien und Daten zu löschen bzw. zu ändern oder selbst per Download zu sichern. Daten bzw. Dokumente wie Arbeitsblätter, Präsentationen, Unterrichtsmitschriften, Ausarbeitungen usw. – „eigene Dateien“ – werden zentral auf der LMS-Instanz der Schule gespeichert.

Hausaufgaben

Hausaufgaben können in digitaler Form über das LMS gestellt, eingereicht und kommentiert werden.

Videokonferenzen

Zur Ermöglichung der Teilnahme am Unterricht auch in Ausnahmesituationen, kann die Lehrkraft einen Konferenzraum über den integrierten Videokonferenzdienst BigBlueButton einrichten.

Die Nutzung des Videokonferenzdienstes zum Distanzlernen bzw. Hybridunterricht darf im Regelbetrieb ausschließlich im Rahmen der über die Schulartenverordnungen zugelassenen Umfänge und Szenarien erfolgen.

Inkrafttreten

Diese Nutzungsordnung tritt am 02. Februar 2026 in Kraft.

Neumünster, den 02. Februar 2026

Der Schulleiter

Hinweise zur Datenverarbeitung im Rahmen der Nutzung des LMS „itslearning“
und
Informationen zum Datenschutz gemäß Artikel 13 der Verordnung (EU) 2016/679 (EU-DSGVO)

Verantwortliche Stelle – behördlicher Datenschutzbeauftragter

Verantwortlich für die Verarbeitung der Daten im Rahmen der Nutzung der Schul-Instanz des LMS ist folgende Stelle:

Holstenschule Neumünster
Altonaer Str. 40
24534 Neumünster

Den Datenschutzbeauftragen für die öffentlichen Schulen erreichen Sie unter:
DatenschutzbeauftragterSchule@bimi.landsh.de, Telefon: 0431/ 988-2452

Zweck und Rechtsgrundlage der Verarbeitung

Die Daten werden zum Zweck (Art. 30 Abs. 1 S. 2 lit b DSGVO) der Bereitstellung und Nutzung eines Lernmanagementsystems (LMS) zum Zugriff auf Unterrichtsmedien, Bereitstellung von Selbstlernaufgaben, Unterrichtsunterstützung usw. verarbeitet.

Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch die Schule sind Art. 6 Abs. 1 e DSGVO i.V.m. § 30 Abs. 1 und ggf. 2a SchulG SH i.V.m. § 4 und ggf. § 12 SchulDSVO. Die Verarbeitung erfolgt zur Erfüllung des schulischen Bildungs- und Erziehungsauftrags gem. §§ 4 und 4 a SchulG SH. Die Verarbeitung im Rahmen der Auftragsverarbeitung ist nach Maßgabe des § 12 SchulDSVO zulässig.

Der Datenumfang im pädagogisch genutzten automatisierten Verfahren wird begrenzt durch die Regelungen in § 11 Abs. 4, 5 SchulDSVO.
Rechtsgrundlage für die Verarbeitung der Lehrkraftdaten sind Art. 6 Abs. 1 e, 88 Abs. 1 DSGVO i.V.m. § 3 Abs. 1, § 15 Abs. 1 LDSG SH ggf. i.V.m. § 85 Abs. 1 LBG SH.

Schutz vor unbefugtem Zugriff

Jedes Benutzerkonto des LMS ist gemäß den Vorgaben der Nutzungsordnung durch ein Passwort gegen Missbrauch – wie beispielsweise die Einsichtnahme und Nutzung durch unbefugte Dritte – geschützt. Eine Weitergabe des Passworts ist unzulässig.

Konten mit Administrationsrechten werden zusätzlich durch einen zweiten Faktor geschützt. Administrationsrechte dürfen keinesfalls dazu verwendet werden, sich ohne Erfordernis Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen (siehe „Protokollierung“ – gesetzlich geregeltes Vorgehen im Fall von Verstößen).

Datenverarbeitung (personen- und nutzungsbezogene Daten)

Für die pädagogisch-didaktische Nutzung des LMS dürfen zu Verwaltungszwecken von den Schülerinnen und Schülern ausschließlich Name, E-Mail-Adresse und die Zugehörigkeit zu einer bestimmten Klasse oder Lerngruppe verarbeitet werden (siehe § 11 Abs. 4 SchulDSVO).
Im Rahmen der pädagogisch-didaktischen Nutzung erfolgt zusätzlich die Verarbeitung von nutzungsbezogenen Daten wie bspw. hochgeladene Dokumente in Kursen, Textbeiträge in Chats, Nachrichten und Kalendern, Teilnahme an Videokonferenzen sowie Aktivitäten im System (siehe „Protokollierung“).

Empfänger der Daten
Intern Zugriffsberechtigte:

- Schülerinnen und Schüler (SuS) auf eigene Daten
- SuS auf Kommunikationsdaten mit anderen SuS/ Lehrkräften
- Lehrkräfte im Sinne des § 34 SchulG (LK) auf eigene Daten
- LK auf Daten der unterrichteten SuS
- Schulleitung/ Administration auf alle Benutzerdaten
- SuS auf Namen der SuS der eigenen Lerngruppe
- LK auf Namen der unterrichteten SuS, LK der eigenen Schule und LK aus Arbeitsgruppen
- Videokonferenz-Gäste (Eltern, Mitarbeitende der Schule) auf die entsprechend temporär entstehenden Kommunikationsdaten
- Weiteres pädagogisches Personal nach Maßgabe der Schulleitung

Extern Zugriffsberechtigte:

- itslearning und dessen Unterauftragsverarbeiter im Rahmen der Auftragsverarbeitung zur technischen Bereitstellung und zum Betrieb der Lernplattform

Kommunikationsdaten
Das LMS wird allein für den Austausch von Informationen im schulischen Zusammenhang bereitgestellt. Die Schule ist damit kein Anbieter von Telekommunikation im Sinne von § 3 Nr. 1 Telekommunikationsgesetz. Ein Rechtsanspruch der Nutzerinnen und Nutzer auf den Schutz der Kommunikationsdaten im Netz besteht gegenüber der Schule somit grundsätzlich nicht. Die Schule ist berechtigt, im Falle von konkreten Verdachtsmomenten von missbräuchlicher oder strafrechtlich relevanter Nutzung des Systems – und ausschließlich in diesem Falle – die Inhalte von Nachrichten zur Kenntnis zu nehmen. Die betroffenen Nutzerinnen und Nutzern werden hierüber unverzüglich informiert.

Protokollierung
Im Rahmen der Nutzung des LMS werden Logins bzw. Zugriffe durch Nutzerinnen und Nutzer (mit Datum und Uhrzeit der letzten Anmeldung) automatisiert protokolliert.
Diese Protokolle dienen der Sicherstellung des ordnungsgemäßen Betriebs und Nutzung des Systems. Zur Gefahrenabwehr werden diese Zugriffsprotokolle gespeichert und nach maximal sechs Monaten automatisiert gelöscht.

Im Fall des Verdachts der unzulässigen Nutzung des LMS, insbesondere im Fall des Verdachts auf Straftaten oder Ordnungswidrigkeiten hat die Schulleitung an erster Stelle zu prüfen, ob die Strafverfolgungsbehörden einzuschalten sind. Die Schulleitung entscheidet im jeweiligen Einzelfall zudem – ggf. in Absprache mit den Strafverfolgungsbehörden -, ob und welche Maßnahmen zur Aufklärung des Vorgangs ergriffen werden (wie bspw. Auswertung der System-Protokolldaten, Auswertung der im Zusammenhang mit der Internetnutzung entstandenen Protokolldaten).
Sollten die Protokolldaten im Verdachtsfall und zum Nachweis unzulässiger Aktivitäten (bspw. Mobbing) an der Schule ausgewertet werden, ist die Schulleitung für eine ordnungsgemäße Einsicht und Auswertung mindestens nach dem Vier-Augen-Prinzip verantwortlich.

Speicherdauer und Löschfristen
Nutzerinnen und Nutzer haben die Möglichkeit, jederzeit selbst Dokumente aus der persönlichen Dateiablage zu löschen. Eigene Dokumente, die zur Nutzung im LMS erhalten bleiben sollen, sind aufgrund der zentralen Speicherung über die Dateiablage der Schule verfügbar.

Die Löschung der auf den Servern des LMS gespeicherten Dokumente und Daten erfolgt grundsätzlich regelmäßig zum Ende des Schuljahres durch die Schule. Daten in der eigenen Dateiablage sind hiervon nicht

betroffen. Ein Benutzerkonto – inklusive aller zugehöriger Daten und Dateien – wird am Ende der Schul- oder Dienstzeit bzw. bei Wegzug aus dem Bundesland Schleswig-Holstein gelöscht. Die Nutzerinnen und Nutzer haben vor der Löschung selbst dafür Sorge zu tragen, eigenständig eingestellte Daten und Dateien aus der persönlichen Dateiablage durch Download für eine mögliche weitere Nutzung zu sichern (Backup).

Darüber hinaus gelten die in der Landesverordnung über die Verarbeitung personenbezogener Daten an öffentlichen Schulen (Schul-Datenschutzverordnung – SchulDSVO) in den §§ 10,15 festgelegten Löschfristen. Alle anderen personenbezogenen Daten werden unverzüglich gelöscht, sofern sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet werden, nicht mehr erforderlich sind (§ 10 Abs. 1 Satz 6). Das Löschkonzept der Schule legt die Verantwortlichkeiten und die Löschfristen im System fest.

Hinsichtlich der im Auftrag verarbeiteten Daten gilt die im Auftragsverarbeitungsvertrag festgelegte Löschung: Die Daten beim Auftragnehmer werden nach Artikel 28 Abs. 3 Buchstabe e spätestens mit Beendigung der Auftragsverarbeitung gelöscht. Sicherungsdateien können noch bis zu 6 Monate über das Vertragsende hinaus Daten enthalten.
Die Speicherung bzw. Löschung folgender personenbezogene Daten basiert zudem auf folgenden Regelungen:

- Stammdaten der Nutzerinnen und Nutzern (Vor- und Nachname, Benutzername, Schul- sowie Klassen- bzw. Lerngruppenzugehörigkeit) werden zentral aus dem Schulportal SH übermittelt. Die Nutzung dieser Daten erfolgt auf Basis der gesetzlichen Vorgaben und ist durch eine Vereinbarung zur Auftragsverarbeitung gemäß DSGVO geregelt.
- Log-Dateien (sogenannte Protokolle; vom Server protokolliert, z.B. IP-Adresse, Betriebssystem und Browser des Rechners, Art der Zugriffe) sind erforderlich für die Sicherstellung der Betriebsbereitschaft und Sicherheit, wie bspw. auch für das frühzeitige Erkennen von möglichen Angriffen auf das System. Darüber hinaus werden Teile dieser Daten verwendet, um Darstellung und Funktionen des LMS korrekt an die Endgeräte der Nutzerinnen und Nutzern auszuliefern.
- Die Verarbeitung nutzungsbezogener Daten (Pädagogische Prozessdaten; schülerbezogene Ergebnisse von Tests, bearbeitete Aufgaben usw.) ist für die Erfüllung des Zwecks der unterrichtlichen Nutzung des Lernmanagements erforderlich. Die Daten dieser Kategorie werden seitens der Schule in der Regel am Ende eines jeden Schuljahres gelöscht. In begründeten Ausnahmefällen ist das Ausweiten der Löschfrist zur schuljahresübergreifenden Verwendung von Dateien möglich. Darüber entscheidet letztendlich die Schulleitung und weist die zuständige Schul-Administration entsprechend an. Ausnahmefälle sind dementsprechend frühzeitig bei der Schulleitung zu melden.
- Die Verarbeitung (insbesondere Speicherung) von Klassenbuch- oder Notizbuchaufzeichnungen (§ 13 SchulDSVO) ist unzulässig.

Betroffenenrechte
Zu der Verarbeitung der Daten besteht bei Vorliegen der erforderlichen Voraussetzungen jeweils das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. auf Datenübertragbarkeit gemäß den Artikeln 15 bis 18 und 20 der Verordnung (EU) 2016/679 (EU-DSGVO). Außerdem hat eine betroffene Person nach Artikel 22 das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 lit e erfolgt, Widerspruch einzulegen.

Beschwerderecht bei der Aufsichtsbehörde
Wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten rechtswidrig ist, besteht das Recht auf Beschwerde bei der Landesbeauftragten für Datenschutz Schleswig-Holstein, Holstenstraße 98, 24103 Kiel, E-Mail: mail@datenschutzzentrum.de, Tel.: 0431 988 1200.

Nutzungsordnung für den KI-Chatbot „telli“
an der Holstenschule Neumünster

Grundsätze der Nutzung

Mit telli steht den Schulen eine KI-Chatbot-Oberfläche für die unterrichtliche Nutzung zur Verfügung.
Telli ist primär als Werkzeug zur Unterstützung des Lernprozesses gedacht, soll jedoch nicht eigenständiges Denken oder die Erstellung von Inhalten vollständig ersetzen.
Schülerinnen und Schüler erhalten über einen von einer Lehrkraft bereitgestellten Link Zugang zur Chatbot-Oberfläche. Der Zugang ist in ein von der Lehrkraft für den Unterricht vordefiniertes Szenario eingebunden.

Telli bietet unterschiedliche Funktionen und kann für verschiedene schulische Zwecke eingesetzt werden:

- Individuelle Lernhilfe und Unterstützung im Unterricht
- Unterrichtsvorbereitung und Erstellung von Lernmaterialien
- Vorkonfigurierbare Lern-Avatare (Dialogpartner) und Lernszenarien
- Hilfe bei Hausaufgaben
- Vorbereitung auf Klassenarbeiten und Prüfungen
- Allgemeine Unterstützung bei schulischen Aufgaben und Projekten
- Kritische Auseinandersetzung, Lernen und Reflektieren über generative KI

Die Ergebnisse von KI-Tools sind stets kritisch zu hinterfragen. Schülerinnen und Schüler sowie Lehrkräfte sind angehalten, die generierten Informationen auf ihre Richtigkeit, Vollständigkeit und Relevanz zu überprüfen. KI-Tools können Fehler machen, Vorurteilen unterliegen oder veraltete Daten verwenden.

Jeder Nutzer und jede Nutzerin hat ein Recht auf den Schutz seiner oder ihrer personenbezogenen Daten. Ein sorgsamer Umgang mit eigenen und fremden Daten ist bei der Nutzung von KI-Tools unerlässlich. Die Sicherheit und der Schutz personenbezogener Daten dürfen nicht durch leichtsinniges, fahrlässiges oder vorsätzliches Handeln gefährdet werden.

Umgang mit personenbezogenen Daten

- Bei der Nutzung von telli dürfen keine persönlichen Daten (z.B. Namen, Adressen, Geburtsdaten, Telefonnummern oder ähnliches einer Person in den Prompt (Eingabebereich) eingegeben werden.
- Falls reale Situationen im Prompt beschrieben werden müssen, sind alle persönlichen Informationen zu pseudonymisieren, sodass ein Rückschluss auf eine konkrete Person nicht o.W. möglich ist.

Urheberrechtliche Vorgaben

Beim Einsatz von KI-Tools dürfen urheberrechtlich geschützte Materialien, insbesondere Texte (z.B. aus Büchern, Artikeln oder dem Internet), nur dann eingegeben werden, wenn und soweit eine entsprechende Nutzungserlaubnis vorliegt oder die Verwendung auf einer gesetzlichen Grundlage beruht, etwa im Rahmen des § 60 a Urheberrechtsgesetz. Diese Vorschrift erlaubt die Nutzung urheberrechtlich geschützter Werke im schulischen Kontext ohne Zustimmung des Urhebers, sofern die Nutzung nicht kommerziell erfolgt, einem konkreten Unterrichtszweck dient und sich auf einen begrenzten Umfang beschränkt. Sofern keine der genannten Voraussetzungen erfüllt ist, sind ausschließlich eigene Inhalte zu verwenden.

Kennzeichnung von KI-generierten Arbeitsergebnissen

Arbeitsergebnisse, die unter Verwendung von KI-Tools erstellt oder maßgeblich beeinflusst wurden, sind gemäß den festzulegenden innerschulischen Regelungen als solche zu kennzeichnen. Dies dient der Transparenz und der korrekten Bewertung der Eigenleistung. (Vgl. Handreichung „KI@Schule“ des Ministeriums für Allgemeine und Berufliche Bildung, Wissnschaft, Forschung und Kultur Schleswig-Holstein,

Inkrafttreten

Diese Nutzungsordnung tritt am 02. Februar 2026 in Kraft.

Neumünster, den 02. Februar 2026

Der Schulleiter

Informationen über die Verarbeitung Ihrer Daten beim telli-Chatbot gemäß Art. 13 der Datenschutz-Grundverordnung (DSGVO)

1. Verantwortliche Stelle – behördlicher Datenschutzbeauftragter

Verantwortlich für die Verarbeitung der Daten im Rahmen der Nutzung der Online Pinnwand SH (OP.SH) ist folgende Stelle:

Holstenschule Neumünster
Altonaer Str. 40
24534 Neumünster

Verfahrensbetreiber ist das
Ministerium für Allgemeine und Berufliche Bildung, Wissenschaft, Forschung und Kultur
Brunswiker Straße 16-22
24105 Kiel
E-Mail: info@bimi.landsh.de

Der Verfahrensbetreiber übernimmt für die Schulen insbesondere die Aufgabe, die Datensicherheit des Gesamtverfahrens (Anwendung und Server) zu gewährleisten und die Dokumentation vorzuhalten. Die beteiligte Stelle (Schule) verantwortet die rechtskonforme Nutzung vor Ort. Die weitere Aufgabenteilung zwischen Schule/Nutzenden und Verfahrensbetreiber als gemeinsam Verantwortliche i. S. d. Artikel 26 DSGVO ergibt sich aus der ZStVO-Schule.
(https://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=ZtrStSchulV+SH&psml=bsshoprod.psml&max=true)

Den Datenschutzbeauftragten für die öffentlichen Schulen erreichen Sie unter:
DatenschutzbeauftragterSchule@bimi.landsh.de , Telefon: 0431/ 988-2452

2. Zweck und Rechtsgrundlage der Verarbeitung

Der KI-gestützte Chatbot „telli“ steht Lehrkräften und Schülerinnen und Schülern Schleswig-Holsteins für die Nutzung zu unterrichtlichen Zwecken zur Verfügung.
Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch die Schule sind Art. 6 Abs. 1 e DSGVO i.V.m. § 30 Abs. 1 und ggf. 2a SchulG SH i.V.m. § 4 und ggf. § 12 SchulDSVO.
Die Verarbeitung erfolgt zur Erfüllung des schulischen Bildungs- und Erziehungsauftrags gem. §§ 4 und 4 a SchulG SH.
Gemäß § 4 SchulDSVO können Schulen die Daten der betroffenen Personen für die Verwaltungs- und im Rahmen ihrer pädagogisch-didaktischen Tätigkeit verarbeiten. Die Verarbeitung im Rahmen der Auftragsverarbeitung ist nach Maßgabe des § 12 SchulDSVO zulässig. Der Datenumfang im pädagogisch genutzten automatisierten Verfahren wird begrenzt durch die Regelungen in § 11 Abs. 4, 5 SchulDSVO.

3. Welche Daten von telli-Nutzenden werden verarbeitet?

3.1 Datenübermittlung und -protokollierung sowie betroffene Kategorien personenbezogener Daten

Der Zugriff der Lehrkräfte auf „telli“ erfolgt über eine automatische Authentifikation und Autorisierung über den ID-Vermittlungsdienst VIDIS über das Schulportal SH.
Zum Zwecke des Berechtigungsmanagement erfasst VIDIS folgende Daten:

1. Rollenart der Rolle im Schulportal
2. Schulkennung: Dienststellennummer(n)
3. Vorname
4. Nachname
5. Schulportal Benutzername
6. E-Mail-Adresse (nur bei LK)

VIDIS übermittelt an telli Dialog folgenden personenbezogene Daten:

1. Identifikator (16-stellige ID)
2. Rolle (Unterscheidung Lehrkraft/Schüler/-in)
3. Schulidentifikator
4. Gerätedaten
5. IP-Adresse
6. Log-Daten

Der technische Dienstleister für die Dienste von telli erhebt und speichert automatisch Informationen in sogenannten Server-Log-Dateien, die der Browser automatisch an telli übermittelt. Dies sind:

1. Browsertyp und Browserversion
2. verwendetes Betriebssystem
3. Referrer URL
4. Hostname des zugreifenden Rechners
5. Uhrzeit der Serveranfrage
6. IP-Adresse, anonymisiert

Aus Gründen der technischen Sicherheit, insbesondere zur Abwehr von Angriffsversuchen, werden diese Daten vom FWU gespeichert. Nach spätestens sieben Tagen werden die Daten gelöscht, so dass es nicht mehr möglich ist, einen Bezug auf einzelne Nutzende herzustellen; ein Abgleich mit anderen Datenbeständen oder eine Weitergabe an Dritte, auch in Auszügen, findet nicht statt.

Schülerinnen und Schüler erreichen telli ausschließlich über einen QR-Code oder mit einem kurzen Token innerhalb eines von der Lehrkraft bereitgestellten Lernszenarios über https://chat.telli.schule/.

3.2 Datenverarbeitung bei der Interaktion mit Sprachmodellen (LLM)

Bei der Nutzung des KI-Chatbots werden die Eingaben der Nutzerinnen und Nutzer an die angebundenen KI-Modelle zur weiteren Verarbeitung übermittelt. Die eingegebenen Daten werden ausschließlich für die Beantwortung der Nutzereingabe verwendet. Eine dauerhafte Speicherung und die Verwendung zu Trainingszwecken der KI erfolgt nicht.

4. Speicherung und Löschung Ihrer Daten

Benutzerdaten werden zweckgebunden gespeichert und nach Entfallen der Voraussetzung gelöscht.
Eine Lehrkraft löscht die angelegten Chatbots und Inhalte eigenständig, wenn diese nicht mehr benötigt werden.
Die von Schülerinnen und Schülern genutzten Chats werden mit dem Schließen des Browsers gelöscht.
Im Rahmen der Verarbeitungstätigkeit übermittelte sowie erhobene Geräte- und Login-Daten werden nach 7 Tagen automatisch gelöscht.

5. Betroffenenrechte

Bei Vorliegen der erforderlichen Voraussetzungen besteht das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. auf Datenübertragbarkeit gemäß den Artikeln 15 bis 18 und 20 der Verordnung (EU) 2016/679 (EU-DSGVO). Bitte richten Sie Ihre Anfrage an die Schule (siehe Punkt 1).

6. Beschwerderecht bei der Aufsichtsbehörde

Wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten rechtswidrig ist, besteht das Recht auf Beschwerde bei der Landesbeauftragten für Datenschutz Schleswig-Holstein, Holstenstraße 98, 24103 Kiel, E-Mail: mail@datenschutzzentrum.de, Tel.: 0431 988 1200.