IT-Nutzungsordnung der Schule

Berufskolleg Kleve des Kreises Kleve

Stand der Information: 20.08.2025

Präambel

Die nachfolgende Nutzungsordnung stellt wichtige Grundregeln im Umgang mit Computern der Schule durch Schülerinnen und Schüler auf. Die Nutzungsordnung ist gültig für die Schulstandorte Kleve, Goch und Haus Riswick. Insbesondere müssen Schülerinnen und Schüler darauf achten, dass

- mit Computern, Tablets, Notebooks und anderer Hardware der Schule, den dazugehörigen Geräten und dem Schulnetz (LAN und WLAN) sorgfältig umgegangen wird,
- die persönlichen Zugangsdaten für die Computernutzung (Kennwort) geheim gehalten und ausschließlich vom jeweiligen Nutzungsberechtigten verwendet werden,
- fremde Rechte und insbesondere das Urheberrecht beachtet werden, dass Materialien, die von anderen Personen stammen, nicht unberechtigt veröffentlicht werden und dass kein unberechtigter Download von Musikdateien, Spielen etc. erfolgt.
- illegale Inhalte weder veröffentlicht noch im Internet aufgerufen werden,
- persönliche Daten (Name, Geburtsdatum, Personenfotos, Videos) von Lehrkräften, Schülerinnen und Schülern und sonstigen Personen nicht unberechtigt im Internet veröffentlicht werden.

Begriffsdefinitionen

IT-Verantwortliche

Als IT-Verantwortliche gelten die Lehrkräfte Herr Stratenschulte, Herr Grossmeilert, Herr Janßen, sowie die IT-Administratoren Herr Rouenhoff, Herr Sackewitz und Herr Füngers.

Selbstlernzentren

Als Selbstlernzentren werden die Räume 1.1.95 und 6.1.10 (am Standort Kleve) bezeichnet. Diese Räume stehen Schülerinnen und Schülern zur unterrichtlichen Vor- und Nachbereitung zur Verfügung.

Schulstandorte

Standort Kleve
Berufskolleg Kleve des Kreises Kleve
Felix-Roeloffs-Straße 7
47533 Kleve
Telefon: 02821 7447-0

Standort Haus Riswick
Berufskolleg Kleve des Kreises Kleve –
Haus Riswick
Elsenpaß 5
47533 Kleve
Telefon: 02821 7116753

Standort Goch
Berufskolleg Kleve des Kreises Kleve in Goch
Jakobstraße 9
47574 Goch
Telefon: 02823 7444

A. Benutzung der Computer und sonstiger Hardware in der Schule

§ 1 Anwendungsbereich

Die Regelungen des Abschnitts A gelten für die Nutzung der Computer, Computerdienstleistungen und Netzwerke, die von der Schule Berufskolleg Kleve des Kreises Kleve betrieben werden. Hierzu zählen insbesondere die Nutzung der von der Schule gestellten Computer in den Computerräumen und in den Selbstlernzentren sowie die Nutzung zentraler Server-Dienste der Schule und die Nutzung der Schulplattform Logineo. Ebenso gilt dies für Tablets und Notebooks sowie interaktive Tafeln. Darüber hinaus gelten die Regelungen für Computer und sonstige netzwerkfähige Endgeräte, die von Schulangehörigen in die Schule mitgebracht werden, soweit sie ihrem Sinn und Zweck nach anwendbar sind.

§ 2 Nutzungsberechtigte

(1) Die in § 1 Satz 1 genannten Computer und Dienste der Schule können grundsätzlich im Rahmen der verfügbaren Kapazitäten von allen Schülerinnen und Schülern unter Beachtung der nachfolgenden Bestimmungen genutzt werden, soweit die Computer nicht im Einzelfall besonderen Zwecken vorbehalten sind. Die Schulleitung oder in Absprache die verantwortlichen Administratoren können weitere Personen zur Nutzung zulassen (z. B. Gäste/Gastschülerinnen/Gastschüler). Die Benutzung kann eingeschränkt, zeitweise versagt oder zeitweise zurückgenommen werden, wenn nicht gewährleistet ist, dass die betreffende Schülerin oder der betreffende Schüler ihren bzw. seinen Pflichten als Nutzerin / Nutzer nachkommen wird oder nachgekommen ist.

(2) Die nutzungsberechtigten Schülerinnen und Schülern haben sich den aufsichtführenden Personen gegenüber auf Verlangen zu legitimieren. Hierzu dienen Schülerausweis und Personalausweis.

§ 3 Zugangsdaten

(1) Alle gemäß § 2 berechtigten Schülerinnen und Schüler erhalten für den Zugang zu den Computersystemen der Schule und zum schulischen Netzwerk (LAN u. WLAN) jeweils eine individuelle Benutzerkennung und erstellen ein sicheres, persönliches Kennwort (Zugangsdaten). Mit diesen Zugangsdaten können sie sich an allen Rechnern des pädagogischen Netzes und im WLAN anmelden. Das Computersystem, an dem sich ein Nutzer im Netz angemeldet hat, ist aus Sicherheitsgründen niemals unbeaufsichtigt zu lassen. Nach Beendigung der Nutzung hat sich der Nutzer an dem von ihm gewählten PC-Arbeitsplatz oder seinem mobilen Endgerät ordnungsgemäß abzumelden.

(2) Um die Sicherheit des Systems zu gewährleisten, wählen die Nutzer komplexe Kennworte. Diese müssen aus einer Folge von 10 bis 14 Zeichen bestehen und sowohl Klein-, Großbuchstaben als auch Ziffern und Sonderzeichen enthalten. Für den Zugang zum LAN und zum WLAN sind unterschiedliche Kennworte zu wählen. Nutzungsdaten dürfen in keinem Fall an Dritte weitergegeben werden.

§ 4 Datenschutz der Zugangsdaten

(1) Die im Rahmen der Zuteilung der Zugangsdaten erhobenen persönlichen Daten der Schülerinnen und Schüler (z. B. Name, Klassenzughörigkeit) werden von Seiten der Schule nicht an Dritte weitergegeben, es sei denn, die Weitergabe erfolgt in Erfüllung einer gesetzlichen Verpflichtung (z. B. im Rahmen von strafrechtlichen Ermittlungen); in diesem Falle werden nur solche Informationen weitergegeben, zu deren Weitergabe die Schule gesetzlich verpflichtet ist.

(2) Mit der Anerkennung der Nutzungsordnung erklärt sich der Nutzer – bei minderjährigen Schülerinnen und Schülern in gesetzlicher Vertretung durch zusätzliche Einwilligung einer sorgeberechtigten Person – einverstanden, dass die Schule berechtigt ist, seine persönlichen Daten im Rahmen der geltenden Datenschutzbestimmungen zu speichern. Dies gilt insbesondere für die Verarbeitung der Daten in der Schulplattform Logineo und im Modul Moodle (siehe Anhang 2).

§ 5 Kennwortweitergabe

Die Schülerinnen und Schüler sind verpflichtet, ihr Kennwort geheim zu halten. Dieses darf nicht an andere Personen weitergegeben werden und ist vor dem Zugriff durch andere Personen geschützt aufzubewahren. Die für die Computernutzung in der Schule verantwortliche Person ist unverzüglich zu informieren, sobald dem Nutzer bekannt wird, dass sein Kennwort unberechtigt genutzt wird. Die Schulleitung ist berechtigt, die Zugangsdaten eines Nutzers unverzüglich zu sperren, wenn der begründete Verdacht besteht, dass das Kennwort durch unberechtigte Personen genutzt wird; die betroffene Nutzerin, der betroffene Nutzer wird hierüber informiert und setzt sich selbst ein neues Kennwort, soweit sie oder er nicht selbst zu dem Missbrauch beigetragen hat.

§ 6 schulorientierte Nutzung

Die schulische IT-Infrastruktur (z. B. schulische Computersysteme, Internetzugang, Software, Peripheriegeräte wie Drucker oder Scanner) darf nur für schulische Zwecke genutzt werden. Als Nutzung zu schulischen Zwecken ist neben Arbeiten im Rahmen des Unterrichts, sowie der Vor- und Nachbereitung des Unterrichts, auch die Nutzung zum Zwecke der Ausbildungs- und Berufsorientierung und der politischen, zeitgeschichtlichen, technischen oder sprachlichen Weiterbildung sowie ein elektronischer Informationsaustausch anzusehen, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit der schulischen Arbeit im Zusammenhang steht. Im Schulnetz dürfen nur schulische Inhalte gespeichert werden. Diese Inhalte können jederzeit vom Lehrpersonal eingesehen werden.

§ 7 Gerätenutzung

(1) Die Bedienung der von der Schule gestellten stationären oder portablen Computer einschließlich jedweder Hard- und Software hat entsprechend den Anweisungen der IT-Verantwortlichen zu erfolgen.

(2) Gegenüber den nach § 2 nutzungsberechtigten Schülerinnen und Schülern, die die Geräte entgegen den Instruktionen und Anweisungen der aufsichtführenden Person nutzen, können geeignete Aufsichtsmaßnahmen ergriffen werden, damit die Betriebssicherheit aufrechterhalten bzw. wiederhergestellt werden kann. In Betracht kommt insbesondere die Untersagung der weiteren Nutzung der Geräte auf Dauer oder für einen bestimmten Zeitraum.

(3) Die Schülerinnen und Schüler sind zum sorgsamen Umgang mit den von der Schule gestellten Geräten verpflichtet. Insbesondere sind die Computertastaturen vor Beschmutzungen oder Kontaminierung mit Flüssigkeiten zu schützen. Das Essen und Trinken während der Nutzung der von der Schule gestellten Computer ist untersagt.

(4) Nach Beendigung der Nutzung muss der Raum ordnungsgemäß verlassen werden. Dabei ist jeder Nutzer für seinen Arbeitsplatz verantwortlich (PC ordnungsgemäß herunterfahren, Gerät/Monitor ausschalten, Arbeitsplatz aufräumen, Stuhl ordentlich an den Tisch stellen. Fenster schließen).

(5) Kabelgebundener Anschluss von fremden Endgeräten an das pädagogische Netz ist untersagt.

(6) Im Gegensatz zu Abschnitt 5 ist die Nutzung privater Endgeräte im WLAN für pädagogische Zwecke im Sinne des BYOD-Konzeptes gestattet. Diese Geräte müssen selbst mit dem WLAN verbunden werden. Ein Support für schulfremde Hardware existiert nicht.

§ 8 Beschädigung der Geräte

Störungen oder Schäden an den von der Schule gestellten Computern sind der aufsichtführenden Person oder der für die Computernutzung verantwortlichen Person unverzüglich zu melden. Die vorsätzliche Beschädigung von Geräten und Einrichtung ist strafbar und kann zur Anzeige gebracht werden. Wer schuldhaft Schäden verursacht, hat diese zu ersetzen. Darüber hinaus kann der handelnden Person die weitere Nutzung dieser Geräte auf Dauer oder für einen bestimmten Zeitraum untersagt werden.

§ 9 Sonstige Einwirkung auf Geräte oder gespeicherte Daten

(1) Veränderungen der Installation und Konfiguration der von der Schule gestellten Computersysteme, Tablets, Notebooks und des Netzwerkes (z. B. durch das Einschleusen von Viren, Würmern oder Trojanischen Pferden) sowie Manipulationen an der schulischen Hardwareausstattung sind untersagt.

(2) Das Ein- und Ausschalten der von der Schule gestellten Computersysteme erfolgt ausschließlich durch die aufsichtführende Lehrkraft bzw. die für die Computernutzung verantwortliche Person oder mit deren ausdrücklicher Zustimmung. Ausnahme hiervon bilden die Selbstlernzentren.

(3) Das Verändern, Löschen, Entziehen oder sonstiges Unbrauchbarmachen von Daten, die auf den von der Schule gestellten Computern von anderen Personen als dem jeweiligen Nutzer gespeichert wurden, ist grundsätzlich untersagt. Automatisch geladene Programme (wie Virenscanner, PC-Wächter) dürfen nicht deaktiviert oder beendet werden.

(4) Die Installation eigener Software – egal in welcher Form – auf den von der Schule gestellten Computern ist nicht zulässig.

(5) VPN Verbindungen/DNS Manipulationen Hard- oder Softwareseitig im pädagogischen Netz sind verboten.

B. Abruf von Internet-Inhalten

§ 10 verbotene Nutzungen

Die gesetzlichen Bestimmungen, insbesondere des Strafrechts, Urheberrechts und des Jugendschutzrechts, sind zu beachten. Das Aufrufen und Verarbeiten sexualisierter, gewaltverherrlichender, jugendgefährdender oder rassistischer Inhalte ist gemäß der Beachtung gesetzlicher Verbotsnormen untersagt. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen und der aufsichtführenden Lehrkraft und den IT-Verantwortlichen unverzüglich Mitteilung zu machen.

§ 11 Download von Internet-Inhalten

(1) Der Down-/Upload, d. h. das Kopieren von Dateien, die in so genannten File-Sharing-Netzwerken angeboten werden, sind sowohl schnurlos als auch schnurgebunden untersagt. Fremde Rechte, insbesondere das Urheberrecht, sind zu beachten; Materialien Dritter dürfen nicht unberechtigt veröffentlicht werden; unberechtigte Downloads (z. B. von Musikdateien oder Spielen) unterbleiben. Auch die Umgehung von Kopierschutzmechanismen ist generell nicht erlaubt. Im Übrigen sind für Kopien die gesetzlichen Schrankenbestimmungen der §§ 44a ff. UrhG zu beachten.

(2) Die Installation von heruntergeladenen Anwendungen auf von der Schule zur Verfügung gestellten Computern ist nicht zulässig.

(3) Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien aus dem Internet, ist zu vermeiden. Sollte eine Nutzerin/ein Nutzer außerhalb schulischer Zwecke oder sonst unberechtigt Daten in seinem Arbeitsbereich ablegen, sind die Schulleitung bzw. die IT-Verantwortlichen berechtigt, diese Daten zu löschen.

§ 12 Online-Abschluss von Verträgen: kostenpflichtige Angebote

Schülerinnen und Schüler dürfen im Rahmen der Nutzung von Internetinhalten weder im Namen der Schule noch im Namen anderer Personen oder selbstverpflichtend Vertragsverhältnisse aufgrund von Angeboten in Informations- und Kommunikationsdiensten eingehen. Ohne Erlaubnis der Schulleitung dürfen des Weiteren keine für die Schule kostenpflichtigen Dienste im Internet in Anspruch genommen werden.

C. Veröffentlichung von Inhalten im Internet

§ 13 Illegale Inhalte

(1) Es ist untersagt, pornografische, gewaltverherrlichende, rassistische, jugendgefährdende, beleidigende oder sonst strafrechtlich verbotene Inhalte im Internet zu veröffentlichen, zu versenden oder sonst zugänglich zu machen. Ferner dürfen Inhalte, die dem Ansehen oder dem Erscheinungsbild der Schule schaden, nicht verbreitet werden.

(2) Kommerzielle und parteipolitische Werbung ist untersagt, soweit die Schulleitung oder eine von ihr autorisierte Person sie nicht im Einzelfall in Übereinstimmung mit den einschlägigen Regelungen zulässt.

§ 14 Veröffentlichung fremder, urheberrechtlich geschützter Inhalte

Texte, (gescannte) Bilder oder sonstige urheberrechtlich geschützte fremde Inhalte (z. B. Audio- und Videodateien) dürfen nur mit Zustimmung des Urhebers oder der sonstigen Rechteinhaber im Internet zum Abruf bereitgestellt, also veröffentlicht werden. Gemeinfreie Werke (insbesondere amtliche Fassungen von Gesetzen, Verordnungen, Erlassen und Bekanntmachungen sowie Werke, bei denen die Schutzfrist abgelaufen ist) dürfen jedoch ohne Erlaubnis im Internet veröffentlicht werden. Ist in einem Einzelfall zweifelhaft, ob Urheberrechte durch eine Veröffentlichung verletzt werden, ist die zuständige Lehrkraft vor der Veröffentlichung zu kontaktieren.

§ 15 Beachtung von Bildrechten

Das Recht am eigenen Bild ist zu beachten. Die Veröffentlichung von Fotos im Internet ist nur gestattet mit der Genehmigung der abgebildeten Personen, im Falle der Minderjährigkeit auch von deren Erziehungsberechtigten.

§ 16 Schulhomepage

Die Veröffentlichung von Internetseiten/Inhalten im Namen oder unter dem Namen der Schule bedarf stets der Genehmigung durch die Schulleitung oder einer durch sie autorisierten Person. Dies gilt auch im Falle von Veröffentlichungen außerhalb der Schulhomepage – etwa im Rahmen von Schul- oder Unterrichtsprojekten.

§ 17 Verantwortlichkeit

Die nach § 2 Nutzungsberechtigten sind für die von ihnen im Internet veröffentlichten Inhalte und Äußerungen innerhalb der gesetzlichen Grenzen (z. B. Vorliegen der Strafmündigkeit ab 14 Jahren; zivilrechtliche Deliktsfähigkeit) verantwortlich, soweit sie nicht glaubhaft machen können, dass ein Missbrauch ihrer Nutzerkennung durch andere Personen – etwa nach vorher vergessener Abmeldung des nach § 2 Nutzungsberechtigten – stattgefunden hat. Gegenüber der verantwortlichen Schülerin oder dem verantwortlichen Schüler können Maßnahmen nach § 2 Satz 3 und § 5 Absatz 1 Satz 3 und 4 ergriffen werden.

§ 18 Bekanntgabe persönlicher Daten im Internet

Schülerinnen und Schülern ist es untersagt, ihre persönlichen Daten (z. B. Telefonnummer, Adresse, E-Mail-Adresse oder ähnliches) oder Personenfotos ohne Einwilligung der aufsichtführenden Lehrkraft oder der IT-Verantwortlichen im Internet, etwa in Chats oder Foren, bekannt zu geben. Davon ausgenommen sind notwendige Angaben zur Anmeldung für schulische Zwecke in Logineo, WebUntis oder Microsoft365.

D. Datenschutz, Fernmeldegeheimnis

§ 19 Aufsichtsmaßnahmen, Administration

(1) Die Schule ist zur Erfüllung ihrer Aufsichtspflicht berechtigt, den Datenverkehr zu speichern und zu kontrollieren. Darüber hinaus können bei der Inanspruchnahme von schulischen Computersystemen oder Netzwerken die zur Sicherung des Betriebs, zur Ressourcenplanung, zur Verfolgung von Fehlerfällen und zur Vermeidung von Missbrauch erforderlichen personenbezogenen Daten elektronisch protokolliert werden. Die für die Administration zuständigen Personen sind berechtigt, zum Zwecke der Aufrechterhaltung eines ordnungsgemäßen Netzwerkbetriebes (z. B. technische

Verwaltung des Netzwerkes, Erstellung zentraler Sicherungskopien, Behebung von Funktionsstörungen) oder zur Vermeidung von Missbräuchen (z. B. strafbare Informationsverarbeitung oder Speicherung) Zugriff auf die Daten der Nutzer zu nehmen, sofern dies im jeweiligen Einzelfall erforderlich ist. Gespeicherte Daten werden in der Regel nach einem Monat, spätestens jedoch zu Beginn eines jeden neuen Schuljahres gelöscht. Dies gilt nicht, wenn Tatsachen den Verdacht eines schwerwiegenden Missbrauchs der schulischen Computer begründen. Die Schule wird von ihren Einsichtsrechten nur in Fällen des Verdachts von Missbrauch und bei verdachtsunabhängigen Stichproben Gebrauch machen.

(2) Die Wahrung des Fernmeldegeheimnisses im Sinne des § 88 TKG wird gewährleistet.

(3) Die IT-Verantwortlichen haben die ihnen im Zusammenhang mit ihrer Tätigkeit für die vorgenannten Systeme bekannt gewordenen Daten geheim zu halten. Zulässig sind Mitteilungen, die zum Betrieb der Rechner und Dienste, zur Erstellung von Abrechnungen, zur Anzeige strafbarer Handlungen und zur Durchführung von Ordnungsmaßnahmen erforderlich sind. Dies gilt auch für das MDM zur Administration von Tablets und anderen schuleigenen Geräten.

(4) Zur Koordination der Unterrichtszeiten von Berufsschule und überbetrieblicher Lehrlingsunterweisung (ÜBL) ist es erforderlich, dass Daten vom Berufskolleg an die ÜBL weitergegeben werden. Durch den Austausch der Daten wird sichergestellt, dass die Unterrichtszeiten der beiden Lernorte so abgestimmt werden können, dass die Teilnahme allen Auszubildenden ermöglicht wird.
Es besteht jederzeit die Möglichkeit, die folgende Einwilligung zur Datenverarbeitung gegenüber der Schulleitung mit Wirkung für die Zukunft zu widerrufen.

(5) Der Benutzerin/dem Benutzer werden innerhalb seiner Dienstzeit/Schulzeit ein Benutzerkonto im pädagogischen Netzwerk sowie eine Microsoft 365 Lizenz zur Verfügung gestellt. Beim Verlassen der Schule wird das Benutzerkonto deaktiviert und gelöscht sowie die Zuweisung der Microsoft 365 Lizenz aufgehoben.
Die Schule sorgt durch technische und organisatorische Maßnahmen für den Schutz und die Sicherheit der im pädagogischen Netz verarbeiteten personenbezogenen Daten. Mit Microsoft wurde zur Nutzung von Microsoft 365 ein Vertrag abgeschlossen, welcher gewährleistet, dass personenbezogenen Daten von Benutzerinnen/Benutzern nur entsprechend der Vertragsbestimmungen verarbeitet werden. Microsoft verpflichtet sich, die personenbezogenen Daten von Benutzerinnen/Benutzern in Microsoft 365 nicht zur Erstellung von Profilen zur Anzeige von Werbung oder Direkt-Marketing zu nutzen.
Ziel unserer Schule ist es, durch eine Minimierung von personenbezogenen Daten bei der Nutzung von Microsoft 365 auf das maximal erforderliche Maß, das Recht auf informationelle Selbstbestimmung unserer Schülerinnen/Schüler und Lehrkräfte bestmöglich zu schützen.
Dieses ist nur möglich, wenn die Benutzerin/der Benutzer selbst durch verantwortungsvolles Handeln zum Schutz und zur Sicherheit ihrer personenbezogenen Daten beizutragen und auch das Recht anderer Personen an der Schule auf informationelle Selbstbestimmung respektieren.
An erster Stelle gilt dieses für die Nutzung von personenbezogenen Daten in der Cloud von Microsoft 365. Es gilt jedoch auch für das pädagogische Netzwerk der Schule.
Personenbezogene Daten gehören grundsätzlich nicht in die Microsoft Cloud, weder die eigenen noch die von anderen! Jede Benutzerin/jeder Benutzer hat dafür zu sorgen, dass Sicherheit und Schutz von personenbezogenen Daten nicht durch leichtsinniges, fahrlässiges oder vorsätzliches Handeln gefährdet werden.
Es besteht jederzeit die Möglichkeit, die Einwilligung zur Datenverarbeitung zur Einrichtung des Microsoft-Kontos gegenüber der Schulleitung mit Wirkung für die Zukunft zu widerrufen. Dadurch erlischt das Recht auf Nutzung dieses Dienstes.

E. Ergänzende Regeln für die Nutzung außerhalb des Unterrichtes

§ 20 Nutzungsberechtigung

(1) Schülerinnen und Schüler dürfen außerhalb des Unterrichts in den Selbstlernzentren die dort aufgestellten Computer nutzen, wenn sie eine Legitimation (§ 2 Abs. 2) bei sich führen.

(2) Ausnahmsweise kann darüber hinaus außerhalb des Unterrichts im Rahmen der medienpädagogischen Arbeit Schülerinnen und Schülern ein weitergehendes Recht zur Nutzung der Schulcomputer und der Netzwerkinfrastruktur gewährt werden. Die Entscheidung darüber und auch in Bezug darauf, welche Dienste genutzt werden können, trifft die Schulleitung.

(3) Der § 6 (schulorientierte Nutzung) bleibt unberührt.

§ 21 Aufsichtspersonen

Als weisungsberechtigte Aufsicht können neben Lehrkräften und sonstigen Bediensteten der Schule, volljährige Schülerinnen und Schüler eingesetzt werden. Sie werden abteilungsweise bestimmt und erfasst.

F. Nutzung von Drittanbieterdiensten

§ 22 Microsoft 365

Der durch die Schule bereitgestellte Drittanbieterdienst Microsoft 365 (siehe §19) unterliegt den gesonderten Lizenzbedingungen/Nutzungsbedingungen der Firma Microsoft Deutschland GmbH. Diese können auf der Herstellerwebseite eingesehen werden.
Auf der Webseite des Berufskolleg Kleve kann das „Verzeichnis der Verarbeitungstätigkeiten“ (VVT) und die „Datenschutz-Folgeabschätzung“ (DSFA) unter dem Stichwort „Datenschutz“ eingesehen werden.

§ 23 KI-Systeme – Langform Anhang 3

(1) Der Einsatz von KI-basierten Sprach- und Textgeneratoren im schulischen Kontext erfolgt ausschließlich zu pädagogischen Zwecken.

(2) Es dürfen keine personenbezogenen Daten von Schülerinnen, Schülern oder Lehrkräften in KI-Systeme eingegeben werden.

(3) Ergebnisse aus KI-Anwendungen sind stets kritisch zu prüfen. Eine Übernahme ohne eigene Reflexion ist nicht zulässig.

(4) Jede Nutzung von KI bei schulischen Arbeiten, Projekten oder Prüfungsleistungen ist kenntlich zu machen. Nicht gekennzeichnete Nutzung gilt als Täuschung im Sinne der Leistungsbewertung (§ 48 SchulG NRW).

(5) Die Schule übernimmt keine Verantwortung für Inhalte, die von externen KI-Diensten generiert werden. Nutzerinnen und Nutzer sind verpflichtet, erstellte Inhalte auf ihre Angemessenheit zu prüfen.

(6) Ein schulischer Zugang zu KI-Systemen kann ausschließlich unter Beachtung der geltenden Datenschutzbestimmungen erfolgen. Private Accounts von Schülerinnen und Schülern dürfen nicht für schulische Zwecke genutzt werden.

(7) Die Nutzung von KI darf nicht zur Erstellung oder Verbreitung unangemessener, diskriminierender oder rechtswidriger Inhalte erfolgen. Verstöße können schulische und rechtliche Konsequenzen haben.

(8) Die Schule behält sich vor, die Installation/Nutzung bestimmter KI-Applikationen auf schuleigenen Endgeräten zu untersagen, z. B. wenn datenschutzrechtliche Bedenken vorliegen.

G. Schlussvorschriften

§ 23 Inkrafttreten, Nutzerbelehrung

(1) Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe durch Aushang (Auslage einer gedruckten Ausgabe im Schulbüro) in der Schule in Kraft. Alle nach § 2 Nutzungsberechtigten werden über diese Nutzungsordnung unterrichtet. Einmal zu jedem Schuljahresbeginn findet eine Unterweisung hinsichtlich der Inhalte der Nutzungsordnung statt, die im Klassenbuch protokolliert wird.

(2) Die nach § 2 nutzungsberechtigten Schülerinnen und Schüler, im Falle der Minderjährigkeit außerdem ihre Erziehungsberechtigten, versichern durch ihre Unterschrift (siehe Anhang 1), dass sie diese Nutzungsordnung anerkennen. Dies ist Voraussetzung für die Nutzung.

§ 24 Verstöße gegen die Nutzungsordnung

Schülerinnen und Schüler, die unbefugt Software von den Arbeitsstationen oder aus dem Netz kopieren oder verbotene Inhalte nutzen, können gegebenenfalls zivil- oder strafrechtlich verfolgt werden. Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung für das Netz und die Arbeitsstation schulordnungsrechtliche Maßnahmen zur Folge haben.

§ 25 Haftung der Schule

(1) Es wird keine Garantie dafür übernommen, dass die Systemfunktionen den speziellen Anforderungen des Nutzers entsprechen oder dass das System fehlerfrei oder ohne Unterbrechung läuft.

(2) Aufgrund der begrenzten Ressourcen können insbesondere die ständige Verfügbarkeit der Dienstleistungen sowie die Integrität und die Vertraulichkeit der gespeicherten Daten ungeachtet der sich aus § 20 ergebenden Pflichten nicht garantiert werden. Die Nutzer haben von ihren Daten deswegen Sicherheitskopien auf externen Datenträgern unter Aufsicht der aufsichtführenden Lehrkraft anzufertigen.

(3) Die Schule haftet vertraglich im Rahmen ihrer Aufgaben als Systembetreiber nur, soweit ihr, den gesetzlichen Vertretern, Erfüllungsgehilfen oder Dienstverpflichteten ein vorsätzliches oder grob fahrlässiges Verhalten zur Last fällt. Im Falle leichter Fahrlässigkeit ist eine Haftung bei Vermögensschäden hinsichtlich mittelbarer Schäden, insbesondere Mangelfolgeschäden, unvorhersehbarer Schäden oder untypischer Schäden sowie entgangenen Gewinns ausgeschlossen.

§ 26 Änderung der Nutzungsordnung, Wirksamkeit

(1) Die Schulleitung behält sich das Recht vor, diese Nutzungsordnung jederzeit ganz oder teilweise zu ändern. Über Änderungen werden alle Nutzer durch Aushang (ggf. zusätzlich per E-Mail) informiert. Die Änderungen gelten grundsätzlich als genehmigt, wenn die jeweilige Nutzerin/der jeweilige Nutzer die von der Schule gestellten Computer und die Netzinfrastruktur nach Inkrafttreten der Änderungen weiter nutzt. Werden durch die Änderungen Datenschutzrechte oder sonstige erhebliche persönliche Rechte der Nutzerinnen/Nutzer betroffen, wird erneut die schriftliche Anerkennung der geänderten Nutzungsbedingungen bei den Nutzern eingeholt. Bei Änderungen der Nutzungsordnung, welche die Rechte minderjähriger Nutzer beeinträchtigen, wird in jedem Fall die Einwilligung der sorgeberechtigten Personen eingeholt.

(2) Sollten einzelne Bestimmungen dieser Nutzungsordnung ganz oder teilweise unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

Anhang 1 – Anerkennung der IT-Nutzungsordnung Berufskolleg Kleve

Schriftliche Anerkennung der IT-Nutzungsordnung und Einwilligung in die Verwendung personenbezogener Daten

Die aktuelle IT-Nutzungsordnung ist auf der Schulwebseite www.berufskolleg-kleve.de in elektronischer Form sowie im Schulbüro in gedruckter Form einsehbar.

Ohne die schriftliche Zustimmung kann kein Zugang zum Schulnetzwerk erfolgen!

1. Hiermit erkläre(n) ich/wir, die IT-Nutzungsordnung der Schule „Berufskolleg Kleve des Kreises Kleve“ vom 08.07.2024 vollständig gelesen zu haben und einschließlich der darin enthaltenen Bestimmungen über den Datenschutz und das Fernmeldegeheimnis durch Unterschrift anzuerkennen.

2. Darüber hinaus willige(n) ich/wir in die in §4 und §19 der Nutzungsverordnung genannte Verwendung von personenbezogenen Daten (Name, Vorname, Ausbildungsberuf, Ausbildungsjahr) ein. Sollte keine Aufnahme in die Schule erfolgen, oder die Schule im weiteren Verlauf verlassen werden, verliert diese Erklärung automatisch ihre Gültigkeit!

Angaben zur Person:

Vorname _____

Nachname _____

Klasse (z. B. KHBGO09A) _____

Geburtsdatum (TT.MM.JJJJ) _____

Unterschrift der Schülerin/des Schülers/Erziehungsberechtigten:

Ort, Datum _____

Unterschrift Schüler _____

Unterschrift Erziehungsberechtigter _____
(nur bei minderjährigen Schülerinnen und Schülern)

Name Erziehungsberechtigter _____
(in Druckbuchstaben)

Benutzeraktivierung durchgeführt:

Name der Lehrkraft: _____

Datum, Unterschrift der Lehrkraft _____

Anhang 2

Nutzungsordnung der Lernplattform Moodle
Informationen zur Verarbeitung personenbezogenen Daten

Die Nutzung der Lernplattform ist z. T. Bestandteil des Unterrichts aber auch Angebot zur individuellen Übung im außerunterrichtlichen Bereich. Zusätzlich dient sie Lehrkräften sowie dem Schulverwaltungspersonal als Hilfsmittel zur Schulorganisation (LIS).

Der Zugang erfolgt über die Zugangsdaten des Intranet's der Schule (LOGINEO).

Über die in der Anmeldung angegebenen, teils automatisch anfallenden, teils vom Nutzer zusätzlich eingegebenen Informationen hinaus protokolliert die der Lernplattform zugrunde liegende Software „Moodle" in einer Datenbank, zu welcher Zeit welche Nutzer/innen auf welche Bestandteile der Lehrangebote bzw. Profile anderer Nutzer/innen zugreifen. Protokolliert wird ferner unter anderem je nach Ausgestaltung des einzelnen Lehrangebots, ob TeilnehmerInnen gestellte Aufgaben erledigt, ob und welche Beiträge sie in den eventuell angebotenen Foren geleistet, ob und wie sie in Workshops mitgewirkt haben.

Darüber hinaus kann jeder Nutzer auf freiwilliger Basis im persönlichen Profil weitere persönliche Daten erfassen.
Weiter werden auf der Lernplattform ab der Registrierung als Nutzer/in eingegebene oder mit Ihrer Nutzung automatisch anfallende Daten verarbeitet. Dabei handelt es sich um personenbezogene Daten für die die einschlägigen datenschutzrechtlichen Regelungen gelten. Diese verlangen vor allem die eingehende Information über Art und Umfang der Erhebung von personenbezogenen Daten und die Art und Weise ihrer Verarbeitung.

All diese Daten sind nur dem Administrator dieser Moodle-Plattform und dem Leiter, der Leiterin des jeweiligen Kurses zugänglich, nicht jedoch (von Daten im Zusammenhang mit Aufgaben, Workshops und Foren abgesehen) anderen Nutzern/innen. Sie dienen ausschließlich der Durchführung der jeweiligen Lehrveranstaltung bzw. zur Schulorganisation und werden nicht an andere Personen oder Stellen weitergegeben, auch nicht in anonymisierter Form. Eine personenbezogene statistische Auswertung der Daten erfolgt nicht.

Alle Protokolldaten werden nach Beendigung des Kurses, spätestens aber nach 35 Tagen automatisch gelöscht.

Mit der Nutzung von Moodle werden zwei **Cookies** (= kleine Textdateien) auf dem jeweiligen Computer lokal gespeichert.

- Der wichtigste Cookie heißt standardmäßig **MoodleSession**. Sie müssen diesen Cookie erlauben, um zu gewährleisten, dass der Zugriff nach dem Login auf alle Seiten möglich ist und auf die richtige Seite zugegriffen wird. Nach dem Ausloggen bzw. Schließen Ihres Browsers wird dieser Cookie automatisch gelöscht.

- Der andere Cookie dient der Bequemlichkeit, standardmäßig beginnt dieser mit dem Text **MoodleID**. Mit diesem Cookie wird Ihr Username in Form einer RC4-Chiffre in Ihrem Browser gespeichert und bei jedem Kontakt mit unserem Server an uns zurück übermittelt. Es ist damit möglich, dass bei einem neuen Einloggen auf unserem Moodle-Server, der Username bereits automatisch in das Login-Formular eingetragen wird. Sie können diesen Cookie verbieten, müssen dann aber bei jedem Login Ihren Usernamen selbst wieder eingeben. Dieser Cookie hat eine Gültigkeit von **60 Tagen** und wird nach Ablauf dieser Zeit von Ihrem Browser automatisch gelöscht.

Kenntnisnahme und Einverständniserklärung
Mit der ersten Nutzung der Lernplattform hat der Nutzer, die Nutzerin von der bezeichneten Datenerhebung und -verwendung Kenntnis genommen und ist bei weiterer Nutzung damit einverstanden.
Zur Berichtigung, Sperrung oder Löschung von personenbezogenen Daten richten Sie sich an den Administrator: Frank Janssen - frank.janssen@berufskolleg-kleve.de

Diese Information wurde in Anlehnung an die von der Landesakademie für Fortbildung und Personalentwicklung an Schulen zur Verfügung gestellten Materialien (http://lehrerfortbildung-bw.de/sueb/recht/form/ds/unterr/) erstellt.

Anhang 3 - Nutzung von KI-Systemen

Präambel & Geltungsbereich
Das Berufskolleg Kleve des Kreises Kleve ermöglicht die didaktisch sinnvolle Nutzung von KI-Systemen zur Förderung von Medien-, Urteils- und beruflicher Handlungskompetenz. Diese Regelung gilt für Unterricht, Projekte, schulische Systeme sowie Leistungs- und Prüfungsleistungen sämtlicher Bildungsgänge.
Sie betrifft Lernende (minder- und volljährig), Lehrkräfte sowie weitere schulische Akteure.
Maßgeblich sind der Bildungs- und Erziehungsauftrag, die Lernortkooperation mit Betrieben sowie die gesetzlichen Vorgaben.

Zulässige Nutzung & Kennzeichnungspflicht
(1) KI-Systeme dürfen nur auf Anweisung oder mit Erlaubnis der Lehrkraft genutzt werden und ausschließlich zu pädagogischen Zwecken.

(2) Jede inhaltliche Nutzung (Texte, Bilder, Code, Auswertungen usw.) ist transparent zu kennzeichnen: „KI-Unterstützung: [Tool, Version, Datum/Zeit]. Verwendete Prompts/Stichworte: …".

(3) Ergebnisse sind kritisch zu prüfen; eine Übernahme ohne eigene Reflexion ist unzulässig.

(4) Nicht gekennzeichnete oder verbotene KI-Nutzung in Leistungszusammenhängen stellt einen Täuschungsversuch dar (vgl. Leistungsrecht/Prüfungsordnungen).

Prüfungen und Leistungsbewertungen (APO-BK)
Die nicht deklarierte oder untersagte Nutzung von KI in Leistungsnachweisen ist ein Täuschungsversuch mit Folgen nach APO-BK (z. B. § 20) und den einschlägigen schulrechtlichen Vorschriften. Dies gilt auch für Haus- und Projektarbeiten, sofern die Aufgabe keine KI-Nutzung vorsieht oder besondere Kennzeichnung verlangt.

Datenschutz & Datensparsamkeit (DSGVO / SchulG NRW / VO-DV I/II)
(1) Es dürfen keine personenbezogenen Daten über Lernende, Erziehungsberechtigte, Ausbilderinnen/Ausbilder oder Lehrkräfte in externe KI-Dienste eingegeben werden (z. B. Namen, Bilder, Leistungsdaten, Gesundheitsdaten, Bewerbungsunterlagen). Besondere Kategorien i. S. v. Art. 9 DSGVO sind strikt ausgeschlossen.

(2) Verarbeitung personenbezogener Daten erfolgt – sofern überhaupt erforderlich – nur auf einschlägiger Rechtsgrundlage bzw. mit wirksamer Einwilligung und unter Beachtung des Grundsatzes der Datenminimierung. Standard ist Nutzung ohne Personenbezug.

(3) Für Lernende unter 16 Jahren gilt Art. 8 DSGVO (Einwilligungsanforderungen). Private Accounts der Lernenden werden für schulische Zwecke nicht verlangt oder genutzt.

(4) Vor Einführung neuer KI-Dienste prüft die Schulleitung Rechtsgrundlage, Auftragsverarbeitung (Art. 28 DSGVO), etwaige Drittlandübermittlungen, Speicherfristen/Löschung, technische und organisatorische Maßnahmen (Art. 32 DSGVO) und bindet die/den Datenschutzbeauftragte*n ein.

Jugendmedienschutz & Inhalte (JMStV).
(1) Inhalte aus KI-Systemen können fehlerhaft, voreingenommen oder unangemessen sein. Lehrkräfte moderieren die Nutzung; Lernende prüfen Inhalte kritisch.

(2) Unzulässige Inhalte (§ 4 JMStV) und entwicklungsbeeinträchtigende Inhalte (§ 5 JMStV) dürfen nicht erstellt, verbreitet oder angezeigt werden; verfügbare Sicherheits-/Filterfunktionen sind zu nutzen. Verstöße werden unterbunden und dokumentiert.

Urheber-, Prüf- und Verantwortlichkeitsvorbehalt.

(1) KI-Ausgaben begründen keinen Anspruch auf Richtigkeit oder Rechtefreiheit; externe KI-Ergebnisse erfolgen ohne Gewähr.

(2) Nutzende tragen Verantwortung für inhaltliche Angemessenheit, Rechteklärung (Urhebern/Nutzungsrechte) und Quellenangaben.

(3) Die Haftung der Schule richtet sich nach den gesetzlichen Vorschriften; individuelle Amtspflichten bleiben unberührt.

Technik & Konten.
(1) Wenn KI-Dienste schulisch bereitgestellt werden, erfolgt die Nutzung ausschließlich über durch die Schule freigegebene Wege (z. B. schulische Zugänge, datenschutzkonforme Konfigurationen), nicht über private Accounts der Lernenden.

(2) Die Schulleitung verantwortet die Einhaltung des Datenschutzes und kann die Nutzung von Diensten untersagen, wenn rechtliche/technische Anforderungen nicht erfüllt sind.

Melde- und Umgangsverfahren.
Unangemessene oder rechtswidrige KI-Ausgaben sind umgehend der Lehrkraft zu melden; Speicherung/Weitergabe solcher Inhalte ist zu unterlassen. Prüfungsrelevante Verstöße werden nach APO-BK geahndet; weitere pädagogische Maßnahmen bleiben vorbehalten.

Transparente Kommunikation & Fortbildung.
Das Berufskolleg informiert Kollegium, Lernende, Ausbilderinnen/Ausbilder sowie Erziehungsberechtigte über Zweck, Umfang und Grenzen der KI-Nutzung (inkl. Datenschutz-Hinweisen) und fördert Fortbildung zu didaktisch und rechtlich sicherer KI-Nutzung.

Inkrafttreten & Überprüfung.
Diese Regelung tritt am [Datum] in Kraft. Die Wirksamkeit wird mindestens jährlich oder anlassbezogen (z. B. Rechtsänderungen, neue Dienste) überprüft und bei Bedarf angepasst. Zuständig: [Funktion/Name der Schulleitung], Datenschutz: [Kontakt der/des behördlichen Datenschutzbeauftragten].

Hinweis: Grundlage u. a. MSB NRW „Umgang mit textgenerierenden KI-Systemen“ (02/2023), SchulG NRW, APO-BK, DSGVO, JMStV. Dieses Muster dient der Risikominimierung und ersetzt keine individuelle Rechtsberatung.