

NUTZERORDNUNG

Kant-Gymnasiums Spandau

(16.08.2020)

Teil I: Allgemeine Nutzerordnung

Benutzung der Computer und sonstiger Hardware in der Schule

1. Anwendungsbereich

Die Regelungen gelten für die Nutzung der Computer, internetfähige Endgeräte, Computerdienstleistungen und Netzwerke (einschließlich WLAN), die von der Schule bereitgestellt werden. Darüber hinaus gelten die Regelungen für Computer und für sonstige digitale Geräte, die von den Schüler*innen in die Schule mitgebracht werden, soweit sie nach Sinn und Zweck auch auf diese Geräte anwendbar sind.

2. Nutzungsberechtigte

(1) Nutzungsberechtigte sind alle Lehrer*innen und Schüler*innen. Die Schulleitung oder der verantwortliche Administrator kann weitere Personen zur Nutzung zulassen (z.B. Gäste, Eltern). Die Benutzung kann eingeschränkt, (zeitweise) versagt oder (zeitweise) zurückgenommen werden, wenn der betreffende Nutzer seinen Pflichten nicht nachkommt.

(2) Weisungsberechtigte sind der verantwortliche Administrator, unterrichts- bzw. aufsichtführenden Lehrkräfte oder von der Schulleitung beauftragte Personen. Den Weisungen der aufsichtführenden Personen ist unverzüglich Folge zu leisten.

(3) Für die Nutzung im außerunterrichtlichen Bereich gelten die Bestimmungen analog.

3. Zugangsdaten

(1) Alle berechtigten Nutzer erhalten für den Zugang zu den Computersystemen der Schule und zum schulischen Netzwerk jeweils eine individuelle Nutzerkennung und ein Passwort, welches sie bei der Erstanmeldung ändern (Zugangsdaten). Mit diesen Zugangsdaten melden sich die Nutzer an allen zugangsgesicherten Endgeräten der Schule an. Das Endgerät, an dem sich ein Nutzer im Netz angemeldet hat, ist aus Sicherheitsgründen durch diesen niemals unbeaufsichtigt zu lassen und ist bei kurzfristigem Verlassen des Arbeitsplatzes zu sperren. Nach Beendigung der Nutzung hat sich der Nutzer an seinem Computersystem ordnungsgemäß abzumelden. Ebenso erhalten die berechtigten Nutzer einen individuellen Zugang zur Anmeldung bei WebUNITIS/UntisMessenger, Office365 sowie gegebenenfalls dem Lernraum Berlin (siehe Teil II der Nutzungsordnung).

(2) Die Nutzer haben sichere Passworte zu wählen.

(3) Die Nutzer sind für die Aktivitäten, die unter ihren Namen laufen, verantwortlich. Sie sind verpflichtet, ihr Passwort geheim zu halten. Dieses darf nicht weitergegeben werden und ist vor dem Zugriff durch andere Personen geschützt aufzubewahren. Die weisungsberechtigte Person ist

unverzögerlich zu informieren, sobald den Nutzern bekannt wird, dass ihr Passwort unberechtigt durch andere Personen genutzt wird.

(4) Das Arbeiten unter einem fremden Passwort ist untersagt. Wer ein fremdes Passwort erfährt, ist verpflichtet, dies der Schulleitung oder der für die Computernutzung verantwortlichen Person mitzuteilen.

4. Datenschutz der Zugangsdaten

Die im Rahmen der Zuteilung der Zugangsdaten erhobenen persönlichen Daten der Schülerinnen und Schüler (Name und Klassen-/Kurszugehörigkeit) 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). Die Daten werden gelöscht, sobald sie nicht mehr benötigt werden.

5. Gerätenutzung

(1) Die Bedienung der von der Schule gestellten oder von Schüler*innen mitgebrachten privaten stationären oder portablen Computer einschließlich jedweder Hard- und Software hat entsprechend den Anweisungen der Weisungsberechtigten zu erfolgen.

(2) Die Schüler*innen sind zum sorgsamem Umgang mit den von der Schule gestellten Geräten verpflichtet. Das Essen und Trinken während der Nutzung der von der Schule gestellten Computer ist untersagt.

(3) Nach Beendigung der Nutzung muss der Raum ordnungsgemäß verlassen werden (PC ordnungsgemäß herunterfahren, Gerät/Monitor ausschalten, Arbeitsplatz aufräumen, Stuhl ordentlich an den Tisch stellen).

(4) Beschädigung der Geräte sowie Störungen sind dem Weisungsberechtigten unverzüglich zu melden. Die vorsätzliche Beschädigung von Sachen ist strafbar und kann zur Anzeige gebracht werden. Wer vorsätzlich Schäden verursacht, hat diese zu ersetzen.

6. Sonstige Einwirkung auf Geräte oder gespeicherte Daten

Veränderungen der Installation und Konfiguration der von der Schule gestellten Computersysteme und des Netzwerkes sowie Manipulationen an der schulischen Hardwareausstattung sind untersagt. Fremdgeräte dürfen nicht ohne Zustimmung des Weisungsberechtigten genutzt werden. Das Löschen und Manipulieren von fremden Daten ist verboten.

Abruf von Internet-Inhalten

7. Verbotene Nutzungen

Die gesetzlichen Bestimmungen, insbesondere des Strafrechts, Urheberrechts und des Jugendschutzrechts, sind zu beachten. Es ist verboten, pornografische, Gewalt verherrlichende, rassistische oder sonst jugendgefährdende Inhalte (z.B. nach dem Jugendschutzgesetz indizierte oder die Menschenwürde verletzende Inhalte) aufzurufen, zu speichern und zu verbreiten. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen und der verantwortlichen Person unverzüglich zu melden.

8. Download von Internet-Inhalten

(1) Private Downloads, Streaming, Kryptomining und Hosting jeglicher Art über das Schulnetz bzw. den schulischen Internetzugang sind verboten. Dies schließt insbesondere die Verwendung von Peer-to-Peer Netzwerken ein.

(2) Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien aus dem Internet ist zu vermeiden. Sollte ein Nutzer unberechtigt Daten in seinem Arbeitsbereich ablegen, ist die Schule berechtigt, diese Daten zu löschen.

9. Online-Abschluss von Verträgen: kostenpflichtige Angebote

Schüler*inenn dürfen im Rahmen der Nutzung von Internetinhalten weder im Namen der Schule noch im Namen anderer Personen oder im eigenen Namen Vertragsverhältnisse eingehen.

Veröffentlichung von Inhalten im Internet

10. Illegale Inhalte

Es ist untersagt, pornografische, Gewalt verherrlichende, 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. Bei der öffentlichen Wiedergabe von Inhalten sind die urheberrechtlichen Bestimmungen zu beachten.

11. Beachtung von Bildrechten

Es ist untersagt, Daten anderer ohne die Einwilligung der betroffenen Person oder eigene persönliche Daten zu veröffentlichen. Bei Minderjährigen ist stets die Genehmigung der Erziehungsberechtigten notwendig. Das Recht am eigenen Bild ist zu beachten.

Datenschutz, Fernmeldegeheimnis

12. Aufsichtsmaßnahmen, Administration

Die Schule ist zur Erfüllung ihrer Aufsichtspflicht verpflichtet. Dazu kontrolliert der bzw. die Weisungsberechtigte die Bildschirminhalte der Schülerarbeitsplätze. Das ist auch elektronisch möglich. Der Datenverkehr wird protokolliert und bei Verdacht kontrolliert. Darüber hinaus können bei der Inanspruchnahme von schulischen Computersystemen oder Netzwerken personenbezogene Daten protokolliert werden.

Schlussvorschriften

13. Inkrafttreten, Nutzerbelehrung

(1) Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe in Kraft.

14. Verstöße gegen die Nutzungsordnung

Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung für das Netz und die Arbeitsstation schulordnungsrechtliche als auch strafrechtliche Maßnahmen zur Folge haben.

15. 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.

Teil II: Kant-spezifische Nutzerordnung

1. Alle SuS und jeweils max. zwei ihrer Erziehungsberechtigten erhalten einen eigenen Zugang zu **Webuntis** bzw. für den **Untis Messengerdienst**. Dieser Account wird von der Schule administriert und wird bei Abmeldung von der Schule deaktiviert. Schüler*innen haben über die Zugänge Einblick in den individuellen Stundenplan, Lernstoff und Hausaufgaben. Zudem besteht die Möglichkeit, Informationen und Dateien auszutauschen. Chaträume ohne Lehrkräfte können nicht eingerichtet und genutzt werden. Auch Erziehungsberechtigte erhalten über individuelle Zugänge die Möglichkeit, den Stundenplan oder auch Hausaufgaben Ihrer eigenen Kinder einzusehen. Die Schule kann Eltern und Kindern über diesen Weg zeitnah und sehr gezielt Nachrichten zukommen lassen. Mit Zustimmung der Schulkonferenz ist es perspektivisch auch vorstellbar, dass Sie Sprechstunden bei Lehrkräften buchen können, Klassenbucheinträge sowie Klassenarbeitstermine sehen oder Fehlzeiten ihrer Kinder bei Krankheit melden. Eltern müssen die Zugangsdaten sicher und auch für ihre Kinder nicht einsehbar aufbewahren. Schüler*innen erhalten eigene Schülerzugangsdaten. Es besteht die Möglichkeit, dass sich mehrere Erziehungsberechtigte mit unterschiedlichen E-Mail Adressen bei WebUntis anmelden, daher die zwei Zugangsdaten.

Mit der Firma Untis haben wir uns für ein Informationssystem eines zertifizierten europäischen Anbieters entschieden, der die Auflagen der Datenschutzgrundverordnung der Europäischen Union (EU-DSGVO) gewährleistet. Die vollständige Datenschutzerklärung des Anbieters ist beim Anbieter selbst abrufbar (<https://www.untis.at/warum-untis/ueber-das-produkt/datenschutz-und-sicherheit>). Wir weisen ausdrücklich darauf hin, dass die Verwendung von WebUntis freiwillig ist. Sollten Sie auf eine Verwendung verzichten, tragen Sie in diesem Fall bitte dafür Sorge, dass Sie schulische Informationen dennoch erreichen!

2. Dem Kollegium und der Schülerschaft werden durch die Schule für das gemeinsame Arbeiten und Lernen im Unterricht und zu Hause **Microsoft Office 365** (im Folgenden „Office 365“) zur Verfügung gestellt und individuelle Zugänge eingerichtet. Somit besteht für das Kollegium und die Schülerschaft die Möglichkeit, die Programme *Word*, *Excel*, *PowerPoint* zu nutzen, über *Teams* kollaborativ zu arbeiten und Daten auf der eigenen Cloud *OneDrive* abzulegen. Mit den Diensten, Programmen und Apps können unsere Schüler*innen mit Lehrkräften und anderen Schülerinnen und Schülern im Unterricht zusammenarbeiten. Die Programme, Dienste und Apps können Sie auch zu Hause zum Lernen und Arbeiten für die Schule verwenden. Das Speichern von privaten Dateien (z.B. private Bilder und Videos) ist auf der zur Verfügung gestellten Cloud („OneDrive“) nicht erlaubt. Wir vergeben individuelle Benutzernamen. Mit dem Benutzernamen und einem Passwort können sich die Schüler*innen bei Office 365 anmelden. Wenn sie die Schule verlassen oder Office 365 nicht mehr benutzen möchten, wird Ihr Benutzerkonto nach etwa 4-6 Wochen gelöscht. Das Sichern der Dateien und Daten liegt in der eigenen Verantwortung. Falls die Schule die Nutzung der E-Mail-Funktion erlaubt, dürfen keine Massen-Nachrichten (Spam) und/oder anderen Formen unzulässiger Werbung versendet werden. Bei Regelverstößen kann die Schulleitung den Zugang zu Office 365 sperren. Microsoft verpflichtet sich, die personenbezogenen Daten nicht zur Erstellung von Profilen, zur Anzeige von Werbung oder Marketingzwecke zu nutzen. Personenbezogene Daten (z.B. Lebensläufe, Klassenfotos, Filme, etc.) gehören grundsätzlich nicht in die Microsoft Cloud, weder die eigenen noch die von anderen. Im Rahmen des Unterrichts kann es jedoch vorkommen, dass personenbezogene Daten entstehen. Bei eigenen personenbezogenen Daten und bei denen von anderen haben alle Beteiligten dafür zu sorgen, dass Sicherheit und Schutz von personenbezogenen Daten nicht durch

leichtsinniges, fahrlässiges oder vorsätzliches Handeln gefährdet werden. Das Passwort muss sicher sein und darf nicht einfach erratbar sein. Das Passwort muss aus mindestens 8 Zeichen bestehen, worunter sich eine Zahl, ein Großbuchstabe und ein Sonderzeichen befinden müssen. Nutzer sind verpflichtet, die eigenen Zugangsdaten zum persönlichen Office 365 Konto geheim zu halten und dürfen nicht an andere Personen weiterzugeben. Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist man verpflichtet, sofort Maßnahmen zum Schutz des eigenen Zugangs zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist der schulische Administrator zu informieren. Sollten Schüler*innen in Kenntnis fremder Zugangsdaten gelangen, so ist es ihnen untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Sie sind jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren. Nach Ende der Unterrichtsstunde oder der Arbeitssitzung an einem Rechner bzw. Mobilgerät meldet man sich von Office 365 ab (ausloggen). Mitarbeiter*innen und Schüler*innen am Kant-Gymnasium können Office 365 freiwillig nutzen.

3. Um einen direkten Austausch zu unterrichtlichen Zwecken auch zu ermöglichen, wenn Lehrkräfte und/oder Schülerinnen und Schüler nicht in der Schule zusammenkommen können (z. Bps. in Zeiten von Schulschließungen) nutzen wir eine Videokonferenz-Plattform, um Sitzungen innerhalb der Lerngruppen unter Leitung einer Lehrkraft, Beratung und Unterstützung durch Lehrkräfte in Kleingruppen oder im Vier-Augen-Gespräch zu ermöglichen. Wir nutzen hierfür **Webex** der Firma Cisco. Die Teilnehmer erhalten per Messenger oder Mail eine Meeting ID oder einen Einladungslink, um damit zum angegebenen Zeitpunkt dem Meeting beitreten zu können. Ein individuelles Nutzerkonto ist nicht erforderlich; bei der Videokonferenz kann ein eigener Nutzernamen gewählt werden. Alle Inhalte der Konferenzen bleiben im Kreis der Teilnehmer. Es erfolgt keine Aufzeichnung oder Speicherung durch die Schule oder den Anbieter. Der Mitschnitt der Videokonferenz durch die Teilnehmenden ist untersagt. Jedem Teilnehmer und jeder Teilnehmerin steht es frei, sich auch per Video phasenweise zu zeigen. Bei Nutzung der Videoübertragung müssen die Personen im Kameraerfassungsbereich damit einverstanden sein. Diese Zustimmung erfolgt durch konkludentes Handeln (Aktivierung der Kameras am jeweiligen Gerät). Bei Video-Konferenzen bzw. Video-Unterricht ist mehr Sorgfalt bei der Bestimmung des sichtbaren Umfeldes geboten. Sie sollten daher nur bei entsprechender Erforderlichkeit durchgeführt werden. Eine Teilnahme nur mit der Audiofunktion ist durchaus möglich. Durch die Nutzung des Tools werden Daten über das Internet übertragen (Metadaten wie die IP-Adresse und das eingesetzte Betriebssystem); ein Programm kann dazu auf eigenen Geräten installiert werden, die Teilnahme ist aber auch über Internetbrowser möglich. Cookies werden gesetzt. Webex gibt in seiner Datenschutzerklärung an, wie die Daten verarbeitet werden. Der Anbieter verpflichtet sich, datenschutzrechtliche Bestimmungen einzuhalten. Eine Überprüfung der Einhaltung ist uns als Schule nicht möglich. Bitte nehmen Sie die Datenschutzerklärung des Anbieters zur Kenntnis: <https://gblogs.cisco.com/de/datenschutz-ist-ein-grundrecht-cisco-webex/>

4. Auch eine Lernplattform nutzen wir an unserer Schule. Der **Lernraum Berlin** ist die kostenlose Lernplattform der Senatsverwaltung und steht allen Berliner Schulen zur Verfügung. Sie bietet Schülerinnen und Schülern die Möglichkeit zur Nutzung von Online-Kursräumen für Unterricht und Schulorganisation, Foren, Dateiablagen, interaktive Inhalte, Tests, Lernspiele und Videokonferenzen (hier ebenfalls der Anbieter Webex der Firma Cisco).

5. Das Kant-Gymnasium übernimmt keinerlei Haftung für Schäden an sog. BYOD (bring your own device)-Geräten oder bei Diebstahl.

6. Bei schwerwiegenden Regelverstößen behält sich die Schule Erziehungs- und Ordnungsmaßnahmen bzw. rechtliche Schritte (z.B. Hinzuziehung der Polizei) vor.

7. Die Lehrkräfte entscheiden, ob eigene Geräte (Smartphone, Tablet, Laptop u.ä.) während des Unterrichts genutzt werden dürfen.

8. Foto-, Filmaufnahmen und Audiomitschnitte sind auf dem Schulgelände nur mit Erlaubnis einer Lehrkraft und zu schulischen Zwecken gestattet.

9. Daten sind vorrangig in der Cloud (*OneDrive*) abzulegen. Datensicherungen müssen eigenverantwortlich durchgeführt werden. Für Datenverlust wird keine Haftung übernommen.

10. Sämtliche Mängel oder Störungen an schulischen digitalen Geräten sind unmittelbar der Fachlehrkraft zu melden.

Anerkennung der Nutzerordnung Teil I und Teil II,
Einwilligung in die Verwendung personenbezogener Daten
sowie der Einrichtung der im Teil II genannten Zugänge

für:

[Vorname des Schülers/der Schülerin] [Nachname des Schülers/der Schülerin]

1. Ich/wir habe(n) die allgemeine Nutzerordnung (Teil I) sowie die Kant-spezifische Nutzerordnung (Teil II) vom Kant-Gymnasium-Spandau vom 16.08.2020 zur Kenntnis genommen.
2. Darüber hinaus willige(n) ich/wir in die in Punkt 4 der allgemeinen Nutzungsordnung genannte Verwendung von personenbezogenen Daten ein.

Hinweis: Die Teilnahme an Videokonferenzen bleibt freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile und wir werden in diesem Fall mit Ihnen gerne Alternativen beraten. Diese Einwilligung kann für die Zukunft jederzeit widerrufen werden.

Die Nutzungsordnung vom 16.8.2020 wird gegebenenfalls zukünftig angepasst, erweitert oder in Teilen verändert. Die Schulgemeinschaft wird darüber natürlich informiert. Eine aktuelle Version der Nutzungsordnung finden man auf der schuleigenen Homepage.

Soweit diese Einwilligung nicht widerrufen wird, gilt sie für die Dauer des Schulbesuchs am Kant-Gymnasium. Gegenüber der Schule besteht ein Recht auf Auskunft über Ihre personenbezogenen Daten, ferner haben Sie ein Recht auf Berichtigung, Löschung oder Einschränkung, ein Widerspruchsrecht gegen die Verarbeitung und ein Recht auf Datenübertragbarkeit.

[Ort, Datum]

[Unterschrift des Schülers/der Schülerin]

[Unterschriften der Erziehungsberechtigten]