Kantonsschule Enge
Zürich

Benutzerrichtlinien und Datenschutz für Informatikdienste

I. Angebot und Zugang

[1] Die Kantonsschule Enge betreibt eine Reihe von Informatikdienstleistungen, die den Schulangehörigen zur Verfügung stehen. Dabei wird unterschieden zwischen den Diensten «Intranet» (Stundenplan, Absenzenverwaltung), «KENpunkt» (Lern-, Kommunikations- und Dateiaustauschplattform, Microsoft 365), «Schulnetzwerk» und «Drahtlosnetzwerk» sowie den Computer-Arbeitsplätzen bzw. Computerräumen.

[2] Alle Schulangehörigen erhalten je nach Benutzergruppe mit ihrem Benutzerkonto Zugriffsrechte auf von der Schule betriebene Dienste. Es wird unterschieden zwischen folgenden Benutzergruppen: Schulleitung, Lehrpersonen, Schüler*innen und Verwaltungs-/Betriebspersonal.

[3] Die Computer-Arbeitsplätze in den Arbeitsräumen und Computerzimmern stehen allen Schüler*innen der Kantonsschule Enge, den Freifach-Schüler*innen der Kantonsschule Freudenberg, den Teilnehmer*innen von Veranstaltungen und Kursen der Kaderschule Zürich sowie den Lehrer*innen und dem Personal der genannten Schulen zur Verfügung.

[4] Die Schulleitung regelt den Zugang und die Öffnungszeiten zu den Computer- und Arbeitsräumen. Der Zugang zu den Computerzimmern ist ausserhalb der Unterrichtszeiten nur mit Bewilligung einer Lehrperson oder der Schulleitung gestattet. Über das Reservationssystem online gebuchte Nutzung hat Vorrang.

[5] Die Schulleitung kann weiteren Personen die Benutzung der Anlagen und Dienste gestatten.

[6] Die Schulleitung behält sich das Recht vor, einzelnen Personen den Zugang zu Computer-Arbeitsplätzen zu untersagen, insbesondere nach Fällen von Missbrauch.

[7] Das WLAN und das Schulnetzwerk sind keine öffentlichen Netze im Sinn des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und stehen ausschliesslich Schulangehörigen und speziell von der Schulleitung bezeichneten Personen oder Personengruppen zur Verfügung.

II. Sorgfalt und Meldepflicht

[1] Im Umgang mit der Informatik-Infrastruktur gilt die Sorgfaltspflicht, insbesondere auch gegenüber der Verbreitung von Viren und Spionage- und Schadsoftware.

[2] Benutzer*innen müssen sich an die in den entsprechenden Arbeitsräumen aufgehängten Benutzerordnungen, Weisungen und Richtlinien halten. Weisungen von Lehrpersonen oder dem Verwaltungspersonal ist unverzüglich Folge zu leisten.

[3] Benutzer*innen sind verpflichtet, defekte Geräte oder Störungen dem Informatik-Support umgehend mitzuteilen (support@ken.ch).

[4] Die Zugangsdaten zum eigenen Benutzerkonto sind vertraulich und dürfen nicht mit anderen Benutzer*innen geteilt werden.

[4] Wenn Hinweise oder der Verdacht bestehen, dass das eigene Benutzerkonto missbraucht wurde, ist darüber unverzüglich Meldung an den Informatik-Support und gegebenenfalls an die Schulleitung zu erstatten.

[5] Wenn private Geräte wie Laptops, Mobiltelefone, Tablets etc. mit dem Schulnetzwerk verbunden werden, sind die Benutzer*innen für die Sicherheit der Geräte selbst verantwortlich.

[6] Benutzer*innen sind verpflichtet, auf Ihren Geräten ein Virenschutzprogramm zu installieren und regelmässig zu aktualisieren.

III. Verbote

Ausdrücklich untersagt sind:

[1] Das Verwenden der User-ID einer anderen Person ohne deren expliziten Zustimmung sowie die Weitergabe von eigenen und/oder fremden Passwörtern. Ausgenommen sind die Administratoren.

[2] Alle Tätigkeiten, die den geordneten Betrieb beeinträchtigen, wie beispielsweise das Verändern der Softwarekonfiguration (Betriebssystem und Anwendungen), das Öffnen resp. Modifizieren von Geräten, Manipulationen an der Verkabelung usw.

[3] Das Arbeiten mit und das Abspielen, Abspeichern, Hochladen, Herunterladen, elektronische Versenden sowie Drucken von Materialien mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt.

[4] Auf Schulgeräten das Verwenden von anderer Software als der vorinstallierten, insbesondere auch das Ausführen von Software ab Wechseldatenträgern.

[5] Die Weitergabe von auf der Lernplattform oder in Microsoft 365 freigegebenen Daten an weitere Personen innerhalb oder ausserhalb der Schule ohne die explizite Erlaubnis der Autor*innen.

[6] Die Nutzung der Informatikdienste und -infrastruktur für jegliche kriminelle oder kommerzielle Nutzung.

[7] Die Weitergabe von Zugangsdaten und Passwörtern zu Dienstleistungen, die Schulangehörigen zur Verfügung gestellt werden, an Dritte ohne die explizite Bewilligung der Schulleitung.

[8] Der Missbrauch der Kommunikationsmittel, speziell zur Verbreitung von Schadsoftware, Spam sowie die Sabotage oder die Störung der digitalen Kommunikationskanäle.

[9] Der Anschluss eigener Geräte an Netzwerksteckdosen. Dies gilt insbesondere für Router, Airports und andere Netzwerkgeräte.

IV. Nutzung

[1] Die Nutzung der zur Verfügung gestellten Geräte und des Netzwerks für schulische Zwecke hat Vorrang. Die private, nicht-kommerzielle Nutzung ist erlaubt, sie kann aber durch die Schulleitung beschränkt werden. Für kommerzielle Nutzungen im schulischen Rahmen kann die Schulleitung Ausnahmen bewilligen.

[2] Die Nutzung von ausgeliehenen Geräten und Geräteteilen ist nur der ausleihenden Person gestattet. Benutzer*innen von Leihgeräten haften für Schäden an den Geräten.

[3] Die Nutzung der von der Schule zur Verfügung gestellten Software ist nur gemäss den entsprechenden Lizenzbestimmungen gestattet.

[4] Der Zugang zu Drahtlosnetzwerk und die Nutzung von Druckern sowie Multifunktionsgeräten mit privaten Geräten ist erlaubt. Die Verantwortung für die Sicherheit des eigenen Geräts liegt dabei bei den Benutzer*innen.

[5] Nach dem Austritt aus der Schule ist die Nutzung von durch die Schule lizenzierter Software und Dienstleistungen nicht mehr gestattet. Die entsprechende Software und die Zugangsdaten zu den Dienstleistungen sind innerhalb von drei Monaten zu löschen.

V. Kommunikation

[1] Die Schulleitung und die Lehrpersonen verwenden für ihre offizielle bzw. dienstliche elektronische Kommunikation untereinander sowie mit den Schüler*innen ausschliesslich die von der Schule bzw. dem Kanton Zürich bewilligten Kommunikationskanäle. Verbindliches Standardkommunikationsmittel sind E-

Mails. Es dürfen auch weitere Kommunikationsmittel genutzt werden, sofern sie vom kantonalen Datenschützer bewilligt sind (z.B. MS Teams).

[2] Alle Schulangehörigen sind verpflichtet, ihre E-Mails und Nachrichten regelmässig, aber mindestens einmal täglich zu lesen und innert nützlicher Frist zu reagieren. Wenn Probleme mit dem E-Mail-Konto oder dem Zugang auftreten, sind diese dem Informatik-Support unverzüglich anzuzeigen.

[3] Die Weiterleitung der schulischen E-Mail-Adresse an eine private E-Mail-Adresse ist ausser in Spezialfällen mit Bewilligung der Schulleitung untersagt.

[4] Der Versand von Massen-E-Mails an die Lehrerschaft und Schülerschaft ist ausser mit Bewilligung der Schulleitung untersagt. Der Versand von E-Mails durch eine Lehrperson an eine oder mehrere Schulklassen im Rahmen ihrer Unterrichtstätigkeit oder der Schulorganisation ist gestattet.

[5] Die Schulverwaltung kann in für den Schulbetrieb nötigen Fällen Massen-E-Mails an alle Schulangehörigen oder bestimmte Gruppen von Schulangehörigen zustellen. Dies betrifft insbesondere das Versenden von Informationen über den Schulbetrieb, technische Störungen und Notfälle aller Art.

[6] Schüler*innen einer Klasse dürfen die Klassen-E-Mailadresse ihrer eigenen Klassen für schulische Zwecke verwenden.

[7] Die E-Mailadressen der Benutzer*innen werden nach dem Muster *vorname.nachname@ken.ch* für Lehrpersonen und *vorname.nachname@stud.ken.ch* für Schüler*innen gebildet. Ausnahmen sind in begründeten Fällen möglich.

VI. Private Geräte / Bring-Your-Own-Device

[1] Schulangehörige dürfen sich mit privaten Geräten mit dem Schulnetzwerk verbinden und die darin zur Verfügung gestellten Dienste nutzen sowie ihr Gerät mit entsprechenden Anschlüssen von Beamern, Visualizern, Docks etc. verbinden.

[2] Die Besitzer der privaten Geräte haften selber für ihre Geräte und sorgen für deren Betriebssicherheit und Wartung.

[3] Die Schule stellt Schulangehörigen Lizenzen von Microsoft 365 und Adobe CC zur Nutzung auf Ihren privaten Geräten zur Verfügung.

[4] Die Schule stellt Lehrpersonen nicht-persönliche Arbeitsplätze mit Bildschirm, Tastatur und Maus zum Anschluss an private mobile Computer zur Verfügung. Die nicht persönlichen Arbeitsplätze sind nach Arbeitsende aufzuräumen.

VII. Datenschutz

[1] Es gelten die Bestimmungen der Verordnung über die Information und den Datenschutz vom 28. Mai 2008 bzw. das Gesetz über die Information und den Datenschutz vom 12. Februar 2007.

[2] Schüler*innen bzw. ihre Erziehungsberechtigten sind verpflichtet, Änderungen der Personendaten dem Schulsekretariat innert Wochenfrist zu melden.

[3] Im Intranet sind die Personendaten der Schüler*innen nur für Lehrpersonen und Verwaltungspersonal einsehbar. In Microsoft 365 werden von der Schule im Benutzerkonto nur der Vorname, der Nachname und die Klassenzugehörigkeit sowie wahlweise eine private E-Mailadresse oder eine Mobiltelefonnummer zur Passwortrücksetzung gespeichert. Benutzer*innen können weitere eigene Personendaten erfassen.

[4] Die E-Mail-Adresse und alle privaten Daten im Benutzerkonto werden innerhalb von drei Monaten nach dem Austritt endgültig gelöscht. Ausgenommen von der Löschung sind geschäftsrelevante Daten, die gemäss Informations- und Datenschutzgesetz vom 12. Februar 2007 archiviert werden müssen. Hier gelten die durch das Gesetz festgelegten Fristen. Für die Sicherung der privaten Daten ist die austretende Person selber zuständig.

[5] Die von Schulangehörigen in der persönlichen Cloud «OneDrive for Business» abgelegten Daten und die E-Mails im persönlichen Postfach des E-Mailsystems gehören dem/der Nutzer*in und sind durch den Datenschutz geschützt. Die Administratoren der Schulinformatik greifen auf diese Daten nur mit Zustimmung des Nutzers / der Nutzerin, in Notfällen oder aufgrund von Weisungen durch Schulleitung oder Behörden zu. Alle Zugriffe werden protokolliert.

[6] Die Weitergabe von Personendaten und E-Mailadressen von Schulangehörigen an Aussenstehende ist ohne Bewilligung der betroffenen Personen oder der Schulleitung nicht gestattet.

[7] Die Nutzung der Informatikdienstleistungen wird in den meisten Fällen protokolliert, etwa durch Aufzeichnung von IP-Adressen und Loginzeiten. Beim Verdacht auf Missbrauch kann die Schulleitung eine personenbezogene Auswertung der protokollierten Daten anordnen.

[8] Die Benutzer*innen von BYOD-Geräten sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung der dazu verwendeten Datenträger verantwortlich. Zur Datensicherheit gehört auch das unwiederbringliche Löschen von nicht mehr benötigten Personen- oder Schüler- bezogenen Daten inkl. allfälligen Kopien und Sicherungen auf anderen Systemen.

[9] Personenbezogene Daten von Lehrpersonen und Schüler*innen, die im Rahmen der schulischen Tätigkeit erfasst werden, müssen auf den zur Verfügung gestellten Netzlaufwerken auf dem schuleigenen Server, für Noten und Absenzen im Intranet oder für die Zusammenarbeit zwischen Lehrkräften und Schüler*innen auf dem OneDrive der Schule gespeichert werden. Die Schulleitung sowie die kantonalen Stellen können Ausnahmen anordnen.

VIII. Strafbestimmungen und Schadenersatz

[1] Sämtliche Rechtsvorschriften sind einzuhalten. Dies gilt insbesondere für strafrechtliche Tatbestände wie Gewaltdarstellungen (StGB 135), Pornografische Schriften (StGB 197 Ziff. 1,3), Rassendiskriminierung (StGB 261) und Aufrufe zur Gewalt (StGB 259). Verstösse gegen diese Richtlinien werden gemäss Art. 11 des Disziplinarreglements der Mittelschulen vom 2. Februar 2015 bestraft.

[2] Bei unsorgfältigem Umgang oder bei Verstössen gegen die Verbote gemäss Punkt III kann zudem Schadenersatz gefordert werden.

[3] Die Schule haftet nicht für rechtswidrige Handlungen der Benutzer*innen der Informatikdienstleistungen.

[4] Benutzer*innen haften für alle Schäden, die bei einer fahrlässigen Weitergabe der persönlichen Logindaten an Dritte entstehen.

[5] Benutzer*innen haften für alle Schäden an Leihgeräten.

Die Schulleitung, im Juni 2020