Hans-Grade-Schule

Integrierte Sekundarschule – 09K06
Region Treptow-Köpenick
Sportbetont und Naturwissenschaftlich-Informationstechnische Ausrichtung

Heubergerweg 37 ☏ 030 636 09 61 E-Mail: kontakt@hans-grade-schule.de
12487 Berlin 🖷 030 632 23 629 Internet: www.hans-grade-schule.de

IT-Nutzungsordnung der Hans-Grade-Schule als Teil der Schulordnung; Stand: April 2021

0. Anwendungsbereich

Die Regeln gelten für die Nutzung aller schulischer IT-Geräten und Netzwerke in der Hans-Grade-Schule. Sie gelten auch für mitgebrachte private Geräte, zum Beispiel bei der Nutzung des WLAN[1].

1. Verhaltensregeln

1.1 Alle Nutzer verpflichten sich, die Rechte anderer Personen zu achten.

1.2 Jeder Nutzer erhält im schulischen ISERV-Netzwerk ein Nutzerkonto, bestehend aus einem individuellen Nutzernamen und einem Passwort, welches bei der Erstanmeldung zu ändern ist.

Jede Lehrkraft erhält ein 2. Nutzerkonto durch den Anbieter der Schulhomepage, bestehend aus einem individuellen Nutzernamen und einem Passwort, welches bei der Erstanmeldung zu ändern ist.

Die Nutzerkonten müssen durch ein Passwort gesichert werden. Es ist untersagt, das Passwort anderen Nutzern mitzuteilen.

Hinweise zur Wahl des Passwortes

- Das Passwort sollte mindestens 8 Zeichen und darf bis zu 128 Zeichen enthalten.
- Je länger das gewählte Passwort, desto sicherer ist es gegen Missbrauch.
- Es sollte verschiedene Zeichen, auch Sonderzeichen sowie Groß- und Kleinschreibung beinhalten. Das Passwort sollte keine persönlichen Daten enthalten.
- Es sollte kein Wort sein, das im Wörterbuch zu finden ist.
- Das Passwort sollte niemals gleich sein wie die Benutzer-Identifikation.
- Es sollte bei der Eingabe nicht leicht erkennbar sein.

Gute Passwörter

- enthalten Groß- und Kleinschreibung (Buchstaben a - z und A - Z) und Zahlen (0 - 9)
- enthalten Sonderzeichen (! # $ % ( ) * + , - . / : ; = ? @ [ ] ^ _ { | } ~)
- sind leicht zu merken, damit sie nicht aufgeschrieben werden müssen
  (Beispiel: Abkürzung eines Satzes mit Sonderzeichen: "Mein Passwort lässt sich gut merken" wird zu "$MP&lsgm+")

Bei Verlust oder Verdacht auf Missbrauch ist der Administrator[2] bzw. die verantwortliche Lehrkraft zu informieren und ein neues Passwort zu erstellen.

Die im gemeinsamen Adressbuch eingegebenen Daten in ISERV sind für alle Nutzer sichtbar. Es wird deshalb geraten, so wenig personenbezogene Daten wie möglich von sich preiszugeben.

Das Arbeiten unter fremden Account ist nicht zulässig.

1.3 Alle Nutzer sind verpflichtet, eingesetzte Filter und Sperren zu respektieren und diese nicht zu umgehen.

1.4 Die Nutzer verpflichten sich, die Regelungen des Straf- und Jugendschutzgesetzes sowie das Urhebergesetz zu beachten. Das Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte auf dem Schulserver ist ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten. Werden solche Inhalte

[1] Eine private Nutzung der schulischen IT-Infrastruktur, insbesondere des schulischen Internetzugangs, kann zugelassen werden. Hierbei sind dann allerdings vor allem zwei Punkte zu beachten:
a) Die Schule haftet nicht für die mitgebrachten privaten Geräte (Diebstahl oder Beschädigung).
b) Das „Surfen“ ist erlaubt und unterliegt – durch die Protokollierung als vorgeschriebene Aufsichtsmaßnahme – einer Kontrolle.

[2] Die Administratoren des schulischen Netzwerks sind der Schulleiter, Herr Dr. Schulze und der Hausmeister, Herr Münster.

versehentlich aufgerufen, ist die Anwendung zu schließen und dieses der verantwortlichen Person unverzüglich zu melden.

1.6 Es werden regelmäßig Backups angefertigt. Dennoch ist ein Datenverlust nicht völlig auszuschließen. Wer Dateien auf IServ hochlädt, über IServ versendet oder nutzt, tut dies in eigener Verantwortung. Die Schule übernimmt keine Verantwortung für die Inhalte und die Art gespeicherter Daten. Die Sicherung in IServ gespeicherter Daten gegen Verlust obliegt der Verantwortung der Nutzer.

1.7 Umfangreiche Up- und Downloads sind nicht erlaubt. Ausnahmen sind vorab mit den Administratoren abzusprechen. Der Download von urheberrechtlich geschützten Dateien ist verboten.

Sollte ein Nutzer außerhalb schulischer Zwecke oder sonst unberechtigt Daten in seinem Arbeitsbereich ablegen, ist die Schule berechtigt, diese Daten zu löschen.

1.8 Im Rahmen der Nutzung von Internetinhalten dürfen weder im Namen der Schule noch im Namen anderer Personen oder im eigenen Namen Vertragsverhältnisse eingegangen werden.

1.9 Die Installation oder Nutzung fremder Software auf schuleigenen Geräten durch die Nutzer ist nicht zulässig, sie darf nur von den Administratoren durchgeführt werden.

1.10 Fremdgeräte dürfen nur mit Zustimmung des Weisungsberechtigten genutzt werden.

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

2. Auswertung von und Einsicht in Daten

Die Schule ist zur Erfüllung ihrer Aufsichtspflicht berechtigt, die schulische Internetnutzung zu kontrollieren. Dazu kann der Weisungsberechtigte die Bildschirminhalte der Schülerarbeitsplätze überprüfen. Das ist auch elektronisch möglich.

Des Weiteren werden die besuchten Internetseiten protokolliert. Die Zugangsdaten und protokollierten Internetdaten 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 Zugangsdaten umfassen Namen und Klassenzugehörigkeit, die protokollierten Internetdaten umfassen IP-Adressen sowie Datum und Uhrzeit der Aufrufe. Bei Nutzung innerhalb der IT der Schule wird die Anonymität gegenüber Dritten durch die Nutzung des schuleigenen Proxy-Servers sichergestellt.

Bei der Nutzung privater Geräte im WLAN-Netz wird zusätzlich die Mac-Adresse als Datum erfasst.

Die Daten werden gelöscht, sobald sie nicht mehr benötigt werden. Die Zugangsdaten sowie die Inhaltsdaten werden gelöscht, sobald der Nutzer die Schule verlassen hat, spätestens zu Beginn des darauffolgenden Schuljahres.

Metadaten wie die protokollierten Internetdaten werden nach 2 Wochen gelöscht.

Im Fall des Verdachts der unzulässigen Nutzung der schulischen IT-Geräte und Netzwerke, insbesondere im Fall des Verdachtes auf Straftaten oder Ordnungswidrigkeiten, kann die Schulleitung im erforderlichen Maße folgende Maßnahmen durchführen:

- Auswertung von System-Protokoll-Dateien
- Auswertung der im Zusammenhang mit der Internetnutzung entstandenen Protokolldaten
- Inaugenscheinnahme von Inhalten der E-Mail- und Chat-Kommunikation.

Welche Protokoll- und Nutzungsdaten zur Aufklärung des Vorgangs ausgewertet werden, entscheidet im jeweiligen Einzelfall die Schulleitung.

3. Kommunikation

3.1 E-Mail, Chat und Messenger

Der persönliche E-Mail-Account darf nur für die Kommunikation innerhalb der Schule (interner Gebrauch) verwendet werden. Die Schule ist damit kein Anbieter von Telekommunikation im Sinne von § 3 Nr. 6 Telekommunikationsgesetz. Ein Rechtsanspruch der 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 E-Mail-Dienstes die Inhalte von E-Mails zur Kenntnis zu nehmen. Die betroffenen Nutzer werden hierüber unverzüglich informiert. Die Entscheidung über die Kenntnisnahme trifft die Schulleiterin bzw. der Schulleiter. Die Einsicht nimmt dann die Schulleiterin bzw. der Schulleiter zusammen mit dem IT-Betreuer und/oder dem schulischen Datenschutzbeauftragten vor (4 Augenprinzip).

Die schulische E-Mail-Adresse darf nicht für private Zwecke zur Anmeldung bei Internetangeboten jeder Art verwendet werden. Das gilt insbesondere für alle sozialen Netzwerke wie z. B. Facebook oder Google+.

Massen-E-Mails, Joke-E-Mails o. ä. sind nicht gestattet.

Die Rechte anderer sind zu beachten.

Für die Chat- und Messenger-Funktion gelten dieselben Vorgaben wie bei der E-Mail-Nutzung.

3.2 Forum

Für die Forum-Funktion gelten dieselben Vorgaben wie bei der E-Mail-Nutzung. Darüber hinaus sind die Moderatoren der Foren berechtigt, unangemessene Beiträge zu löschen. Die Nutzer verpflichten sich, in Foren, Chats und von IServ aus versendeten E-Mails die Rechte anderer zu achten.

3.3 Kalender

Kalendereinträge für Gruppen werden nach bestem Wissen eingetragen und nicht manipuliert.

3.4 Hausaufgaben

Hausaufgaben können über IServ gestellt werden, müssen aber im Unterricht angekündigt werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum.

4. Rollenkonzept

Die **Administratoren** haben weitergehende Rechte, verwenden diese aber grundsätzlich nicht dazu, sich Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen. Sollte ein Nutzer sein Passwort vergessen haben, ist er verpflichtet, dass durch einen Administrator neu vergebene Passwort beim nächsten Einloggen sofort zu ändern. Nur der Nutzer selbst darf ein neues Passwort für sich persönlich bei einem Administrator beantragen. Chat-Protokolle sind auch für Administratoren grundsätzlich nur lesbar, wenn ein Verstoß per Klick auf der entsprechenden Schaltfläche gemeldet wurde.

Für die Gruppenforen können **Moderatoren** eingesetzt werden, die Forumsbeiträge auch löschen können. Moderatoren dürfen nur in dem ihnen anvertrauten Forum moderieren.

5. Verstöße

Im Fall von Verstößen gegen die Nutzungsordnung kann das Konto gesperrt werden. Damit ist nur noch eine eingeschränkte Nutzung möglich.

6. Eingeschränkte Nutzung

Sollte nicht oder nur mit Einschränkungen in die Nutzung von IServ eingewilligt werden bzw. falls das Konto gesperrt wurde, so treten folgende Möglichkeiten ein:

a) Die Nutzung der schulischen Computer findet mit Hilfe des eingeschränkten Accounts statt. Mit diesem kann sich dann nur noch an den Computern der Schule angemeldet werden.
b) Die Nutzung der schulischen Computer findet mit Hilfe eines lokalen Accounts statt. Bei beiden Möglichkeiten können keine eigenen Daten auf dem System gespeichert und ausgetauscht werden. Die Nutzerin/der Nutzer ist selbst dafür verantwortlich, seine Daten auf einem eigenen Datenträger (USB-Stick) zu speichern. Die Nutzerin/der Nutzer hat dafür zu sorgen, dass keine Schädlingsprogramme sich auf dem USB-Stick befinden. Das Arbeiten mit den Modulen über der Browser-Oberfläche ist nicht möglich.

7. Abschlussbemerkung - Datenschutz

Es gilt die Datenschutzerklärung der Hans-Grade-Schule, die auch online auf der Webseite einzusehen ist.