Fritz-Reuter-Oberschule
(Integrierte Sekundarschule mit gymnasialer Oberstufe)
Berlin, Bezirk Lichtenberg (11K05)

Stand 15. Juni 2023

IT-Nutzungsordnung

Anwendungsbereich

Die Regeln gelten für die Nutzung aller schulischer IT-Geräten und Netzwerke.

Sie finden auch für private Geräte, zum Beispiel für die Nutzung von WLAN, Anwendung[1].

1. Verhaltensregeln

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

1.2 Jeder Nutzer erhält ein **Nutzerkonto**, bestehend aus einem individuellen Nutzernamen und einem Passwort, welches bei der Erstanmeldung zu ändern ist. Das Nutzerkonto muss durch ein nicht zu erratendes **Passwort** von mindestens acht Zeichen Länge (Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen) gesichert werden. Es ist untersagt, das Passwort anderen Nutzern mitzuteilen.

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

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 **gesetzlichen 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 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.

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] 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) Es entstehen Haftungsrisiken für die Schule durch die mitgebrachten privaten Geräte (Diebstahl oder Beschädigung).
b) Die Nutzer müssen informiert werden, inwieweit „privates“ Surfen erlaubt ist und dass das private Surfen durch die Protokollierung als vorgeschriebene Aufsichtsmaßnahme ebenfalls einer Kontrolle unterliegt.
Sollten Zugriffe von außen möglich sein, sind weitere Regelungen erforderlich:

[2] Die Nutzer sind zu informieren, welche Personen an der Schule zuständig sind.

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 I**nstallation oder Nutzung fremder Software** durch die Nutzer ist nicht zulässig, sie darf nur von den Administratoren durchgeführt werden.

1.10 Fremdgeräte dürfen nur mit Zustimmung der Lehrkräfte 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.

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 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. Verstöße

Im Fall von Verstößen gegen die Nutzungsordnung kann die Nutzungsberechtigung entzogen werden. Verstöße können schulordnungs-, zivil- oder strafrechtliche Maßnahmen zur Folge haben.

Mit freundlichen Grüßen

Steer

Herr Steer, Schulleiter