

IKT-Nutzungsvereinbarung

Die Nutzung der IKT (Informations- und Kommunikationstechnologischen) Infrastruktur der Schule und des Internets erfordert ein hohes Maß an Verantwortung.

Die gesamte IKT-Infrastruktur (bestehend aus verschiedenen IKT-Ressourcen wie Computerarbeitsplätzen, Notebooks, Tablets, interaktiven Tafeln, Druckern, W-LANs, etc.) dient ausschließlich unterrichtlichen Zwecken und ist sorgsam zu behandeln. Für ihre Nutzung gelten die **IKT-Richtlinien**:

1. Die IKT-Ressourcen der Schule dienen ausschließlich dem Unterricht bzw. der Unterrichtsvorbereitung.
2. Essen und Trinken bei der Benutzung von IKT-Ressourcen ist verboten, um Verschmutzungen oder Beschädigungen zu vermeiden.
3. Andere dürfen durch die Benutzung einer IKT-Ressource nicht gestört werden.
4. Ein sparsamer und verantwortungsvoller Umgang mit IKT-Ressourcen der Schule (Drucker, Speicherplatz usw.) wird vorausgesetzt. Nach der Verwendung sind elektrische Geräte auszuschalten.
5. Die Nutzung interaktiver Whiteboards (IWB) und Beamer ist nur während der Unterrichtsstunden erlaubt.
6. Unerlaubte Veränderungen an Einstellungen der IKT-Ressourcen (z.B. Umstecken und Abstecken von Kabeln, Öffnen der Computer, Installation von Programmen) sind verboten.
7. Das Speichern von nicht schulbezogenen Daten (z.B. Bilder, Videos, Musik, etc.) ist nicht zulässig.
8. Die Schule ist nicht für das Backup der Daten von Schüler/innen und Lehrer/innen verantwortlich, d.h. wichtige Daten müssen selbständig auf einem eigenen Medium gesichert werden, um beispielsweise bei Störungen nicht verloren zu gehen.
9. Der IT-Systembetreuer ist berechtigt im Bedarfsfall Daten zu löschen.
10. Einträge im elektronischen Klassenbuch sind ausschließlich von Lehrpersonen durchzuführen.
11. Das Weitergeben von Benutzernamen und Passwörtern an andere ist nicht zulässig.
12. Die Verwendung fremder Zugangsdaten (Benutzernamen und Passwörter) ist untersagt. Wem fremde Zugangsdaten bekannt werden, ist verpflichtet dies der Schulleitung bekannt zu geben.
13. Das Umbenennen, Verändern, Verschieben und Löschen von fremden Dateien ist verboten und nur mit Einwilligung des jeweiligen Erstellers/in erlaubt.
14. Die mutwillige Verbreitung von Viren, Malware oder schädlicher Scripts usw. ist verboten, sowie das Erlangen fremder Daten durch entsprechende Tools.
15. Das Einrichten von WLAN-Zugangspunkten (auch am Handy) auf dem Schulgelände ist nur mit Genehmigung erlaubt.
16. Schäden und Störungen der IKT-Infrastruktur sind unverzüglich mitzuteilen.
17. Bei der elektronischen Kommunikation sind keine beleidigenden und diskriminierenden Formulierungen zu verwenden. Cyber-Mobbing Vorfälle, Verunglimpfungen, Verhetzungen, üble Nachrede,

Kreditschädigung, Verleumdungen oder Ähnliches müssen unverzüglich einer Lehrperson mitgeteilt werden.

18. In der Schule dürfen illegale Inhalte nicht heruntergeladen, gespeichert oder weiterverbreitet werden. Dies gilt insbesondere für Internetseiten oder Materialien mit gewaltverherrlichendem, pornographischem, rassistischem oder nationalsozialistischem Inhalt. Verstöße gegen dieses Verbot haben disziplinarische bzw. rechtliche Konsequenzen zur Folge.
19. Das Erstellen von Fotos und Audio- oder Videoaufnahmen auf dem Schulgelände und auf Schulveranstaltungen und insbesondere deren Verbreitung sind nur mit Einwilligung der abgebildeten Personen erlaubt. Für eine Veröffentlichung ist zusätzlich die Einwilligung einer Lehrperson oder der Direktion (bei Minderjährigen auch die der Eltern) einzuholen.
20. Bei Verwendung fremder Inhalte ist insbesondere das Urheberrecht zu beachten.
21. Dem Ansehen der Schule und schulnaher Personen darf in keiner Weise geschadet werden. Dies betrifft auch Aktivitäten – anonym oder namentlich – in sozialen Netzwerken (z.B. Facebook) und im Internet allgemein.
22. Die Schule ist in keiner Weise für den Inhalt der über ihren Internetzugang bezogenen Informationen verantwortlich.
23. Zuwiderhandlungen gegen diese Nutzungsordnung können disziplinarische und rechtliche Folgen haben. Bei Verstößen behält sich die Schule den Widerruf der Nutzungsgenehmigung, Disziplinarmaßnahmen und Schadenersatzforderungen vor.

Passwortsicherheit

Sicher ist ein Passwort, wenn es sowohl von automatisierten Bots, als auch von nahestehenden Personen nur mit extremem Aufwand erraten oder mittels eines Brute-force-Attacks herausgefunden werden kann. Wenn das Passwort folgende Kriterien erfüllt, sollte es einigermaßen sicher sein:

1. Besteht mindestens (!) 8 Zeichen
2. Beinhaltet kein Wort, das in einem Wörterbuch vorkommt.
3. Hat keine Zeichenfolgen, die in einem näheren Zusammenhang mit Ihnen stehen (Geburtsdaten, Haustiernamen...).
4. Enthält mindestens eine Zahl, ein Sonderzeichen und besteht aus Groß- und Kleinbuchstaben.
5. Das Passwort wird nur für je einen Dienst verwendet.

Stand: Sept. 2018

