SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

33 Tipps für den digitalen Schulalltag

Das komplette Material finden Sie hier:

School-Scout.de

Inhaltsverzeichnis

Vorwort 4

Techniktipps
› Sichere Passwörter erstellen 6
› Große Dateien verschicken 9
› Einen WLAN-Hotspot einrichten 11
› Tastenkombinationen verwenden 13
› Die SSK-Regel anwenden 14
› Ein Endgerät spiegeln 15

Tipps für die Unterrichtsplanung
› Cloudbasiert arbeiten 16
› Offene Aufgaben stellen 18
› Präsentationsfolien erstellen 20
› Unterrichtsmaterial im Netz finden 22
› Erklärvideos selbst erstellen 24
› Freie Software nutzen 26

Tipps für die Unterrichtsdurchführung
› Professionell präsentieren 28
› Know-how der Schüler*innen als Ressource sehen 30
› Lernprodukte würdigen 31
› Alternative Leistungsnachweise ermöglichen 33
› Schüler*innen Audio-Feedback geben . 35
› Feedback digital einholen 37

Kommunikationstipps
› E-Mail-Pingpong vermeiden 39
› Videokonferenzen gestalten 41
› E-Mails schreiben 43
› Mit Eltern / Erziehungsberechtigten kommunizieren 45

Organisationstipps
› Termine digital organisieren 47
› To-dos digital organisieren 49
› Einen gemeinsamen Termin finden . . . 51
› Das E-Mail-Postfach leer räumen 53

Tipps für die Herausforderungen der digitalen Welt
› Urheberrecht beachten – Beispiel Bildmaterial 55
› Persönliche Daten schützen und sichern 57
› Cybermobbing begegnen 60
› Fake News thematisieren 62

Tipps für die eigene Professionalisierung
› Ein virtuelles persönliches Lernnetzwerk aufbauen 64
› Digitale Fortbildungsangebote nutzen . 66
› Konferenzen, Barcamps & Co. besuchen 68

Vorwort

Digitaler Schulalltag

Der schulische Alltag hat sich in den letzten Jahren verändert. Digitale Medien haben Einzug gehalten in Unterricht und Schule. So werden zum Beispiel die Unterrichtsplanung, -durchführung und -nachbereitung zunehmend digital organisiert. Aber auch die Kommunikation und Kollaboration im Kollegium, mit Eltern / Erziehungsberechtigten und Schüler*innen wird zunehmend digitaler. Kurzum: Der Workflow der Lehrkräfte befindet sich in einem grundlegenden Wandel. Durch die Corona-Pandemie wurden diese Prozesse noch beschleunigt. Digitale Medien waren plötzlich Voraussetzung dafür, dass Unterricht (als Distanz- oder Hybridunterricht) überhaupt durchgeführt werden konnte.

Die vorliegende Tippsammlung versteht sich als Ratgeber für die vielen neuen Möglichkeiten, aber auch Herausforderungen, die durch die Digitalisierung im schulischen Alltag entstehen. So kann der Einsatz digitaler Medien technische Probleme mit sich bringen, rechtliche Fragestellungen aufwerfen oder auch ein Gefühl der Überforderung auslösen aufgrund der Vielzahl an vorhandenen Tools, Methoden und Formaten usw.

Die Tipps geben Antworten auf die häufigsten Fragen, die beim digitalen Arbeiten und im digitalen Unterricht auftreten, und zeigen Wege auf, wie Lehrkräfte digitale Medien sinnvoll und sicher im Schulalltag nutzen können, wie sie Hürden erfolgreich meistern und mögliche Probleme lösen.
Der Autor greift dabei auf seine langjährige Erfahrung als Lehrer, Fortbildner und Mitglied verschiedener Online-Communitys im Bereich „Digitale Bildung" zurück. Alle Tipps sind praxiserprobt und haben sich in verschiedenen Kontexten bewährt.
Es wird jeweils zunächst die Problemlage beschrieben, anschließend wird der entsprechende Tipp anschaulich erläutert. Die Formulierungen wurden stets so gewählt, dass sie für Lehrkräfte, die in das Thema einsteigen und bisher nur wenig Erfahrung im Themenfeld „digitale Medien" gesammelt haben, verständlich sind. Wo sinnvoll, wurden passende Links, Screenshots oder andere visuelle Darstellungen ergänzt.

Vorwort

Haftungsausschluss, datenschutzrechtliche und allgemeine Hinweise

Alle genannten Internetlinks wurden zum Zeitpunkt der Druckfreigabe noch einmal getestet und funktionierten. Es kommt jedoch immer wieder vor, dass einzelne Links abgeschaltet werden oder zu einer anderen Quelle führen. Auch auf den Inhalt und die Aktualität der Internetseiten kann kein Einfluss genommen werden, somit kann auch nicht garantiert werden, dass die Inhalte zu einem späteren Zeitpunkt noch dieselben sind wie zum Zeitpunkt der Drucklegung.

Bei den webbasierten Angeboten ist zu beachten, dass der jeweilige Anbieter, der je nach Serverstandort ggf. nicht den relativ strengen deutschen Datenschutzrichtlinien unterliegt, in der Regel nutzer*innenbezogene Daten sammelt, analysiert und verwertet.
Die Lehrkraft sollte sich deshalb immer vorab in den Datenschutz- und Nutzungsbedingungen der jeweiligen Anbieter über die Bedingungen informieren und ggf. mit der Schule / dem Schulträger klären, ob eine Nutzung im schulischen Kontext gestattet ist.

Für registrierungspflichtige Dienste kann die Schule ggf. E-Mail-Konten für die Schüler*innen bereitstellen, damit diese nicht ihre privaten Adressen verwenden müssen. Falls ein Tool die Eingabe von Namen verlangt, sollten diese auf jeden Fall pseudonymisiert werden. Dies gilt insbesondere für Namen von Schüler*innen.

Die Tipps wurden nach bestem Wissen und Gewissen des Autors erstellt und vielfach erprobt, letztlich aber kann keine Gewähr übernommen werden. Jede Lehrkraft ist verpflichtet, sich über die geltenden Bestimmungen in ihrem Bundesland und an ihrer Schule selbst zu informieren.

Sichere Passwörter erstellen

Beschreibung des Problems

Mit der zunehmenden Fülle von täglich genutzten Plattformen und Apps, die für die Gestaltung des Unterrichts mit digitalen Medien erforderlich sind, geht die Bedeutsamkeit sicherer Passwörter einher. Hier sind wir jedoch nicht selten zu nachlässig.
So habe ich schon des Öfteren von Kolleg*innen gehört, dass sie dasselbe Passwort für verschiedene Zugänge nutzen, da sie sich nicht für jedes Portal ein eigenes Passwort merken können / wollen. Davon ist dringend abzuraten, weil sich so potenzielle Angreifer*innen mit nur einem Passwort Zugriff auf unterschiedliche Inhalte und Kommunikationssysteme verschaffen können.
Eine andere, ebenso verbreitete Angewohnheit ist es, möglichst kurze und oft sogar mit persönlichen Daten (z. B. dem eigenen Vornamen) versehene Passwörter zu verwenden. Auch dies ist nicht zu empfehlen, da die Sicherheit eines Passworts maßgeblich von der Komplexität der Zeichenfolge abhängt.
Auch die Argumentation, man habe nichts zu verbergen und könne deshalb auf möglichst sichere Passwörter verzichten, ist mir in den letzten Jahren mehrfach begegnet. Zu beachten ist aber, dass es nicht nur um die Inhalte geht, die ggf. eingesehen, verändert oder gelöscht werden können, es wird vielmehr auch die Möglichkeit geschaffen, die Kommunikationswege zu kapern und Missbrauch damit zu betreiben.

Tipp

Es gibt mehrere Möglichkeiten, ein sicheres Passwort zu erstellen. Im Folgenden möchte ich zwei Varianten genauer vorstellen.

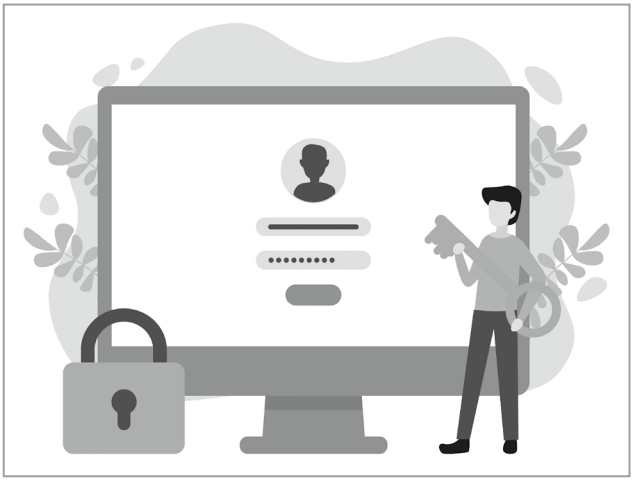
› Verwendung eines Passwortmanagers
Passwortmanager (auch Kennwort- oder Passwortverwaltung) sind kleine Programme, die in der Regel im Browser installiert werden und mit deren Hilfe man komplexe, individuelle Passwörter erstellen, Zugangsdaten verschlüsselt speichern und verwalten kann. Die mit einem Passwortmanager generierten Passwörter können als sehr sicher eingestuft werden. Zudem muss man sich nur ein Passwort merken, eben jenes, welches den Zugang zu dem Passwortmanager erlaubt. Dieses allerdings sollte man auf keinen Fall vergessen, da man sonst auch keinen Zugriff mehr auf die anderen Passwörter hat.
Erwähnt werden soll jedoch auch, dass man sich mit der Verwendung eines Passwortmanagers in die Abhängigkeit von einer Software begibt und auf die Verfügbarkeit und das Funktionieren dieser Software angewiesen ist. Auch können Passwortmanager Ziel von Cyberangriffen sein, was im schlimmsten Fall dazu führen kann, dass alle Passwörter auf einmal abgegriffen werden.

Sichere Passwörter erstellen

› Verwendung eines Passsatzes
Bei dieser Methode formuliert man zunächst einen Satz, den man sich gut merken kann. Dann nimmt man z. B. die Anfangsbuchstaben der einzelnen Wörter dieses Satzes (in Groß- und Kleinschreibung) und fügt schließlich noch Sonderzeichen und Ziffern hinzu, um das Passwort möglichst komplex zu gestalten. Die Zeichenfolge sollte mindestens zehn bis zwölf Zeichen lang sein – je länger, desto besser.
Um nun noch zu vermeiden, dass man für mehrere Anwendungen dasselbe Passwort benutzt, gibt es einen einfachen Trick: Man hängt jeweils ein Suffix an, welches z. B. aus dem ersten und dem letzten Buchstaben der Plattform bzw. App sowie einem Sonderzeichen besteht. Natürlich kann die Zeichenfolge auch an einer anderen Stelle eingefügt werden.

Beispiel
- Als Passsatz habe ich mir *Einem geschenkten Gaul schaut man nicht ins Maul* überlegt.
- Auf die Anfangsbuchstaben verkürzt, ergibt sich: *EgGsmniM*
- Kombiniere ich dies noch mit Ziffern und Sonderzeichen, könnte das Passwort so aussehen: *!1EgGsmniM9?*
- Möchte ich dieses Passwort für ein Mail-Programm verwenden, könnte das Passwort schließlich lauten: *!1EgGsmniM9?M@I*

Darüber hinaus gilt: Wann immer möglich, sollte man die sogenannte Zwei-Faktoren-Authentifizierung (eine zusätzliche Sicherungsebene) nutzen, die immer mehr Anbieter von cloudbasierten Diensten zur Verfügung stellen.



© Natty – stock.adobe.com

SCHOOL-SCOUT.DE

Unterrichtsmaterialien in digitaler und in gedruckter Form

Auszug aus:

33 Tipps für den digitalen Schulalltag

Das komplette Material finden Sie hier:

School-Scout.de