

**Leitfaden zur
„sicheren“ Internetnutzung
für Lehrer/innen
der
allgemein bildenden Pflichtschulen**

Erstellt vom pädagogischen IT-Beirat

des SSRfWien/APS:

HObln Andrea Fleischmann

HD Bernhard Heinisch

SOBln Martina Hochenauer, MSc

VObl Ernst Karner

VI Josef Resinger, MSc

ObL.PTS Wolfgang Scherzer, MSc

HObl Ing. Christian Schütz, MSc

HObln Helene Swaton

VObln Marianne Tischler

HObln Lydia Tittler

1. Problemaufriss

Durch die stark zunehmende Nutzung des Internets bzw. der verschiedenen Dienste gewinnt das Erreichen einer ausreichenden Medienkompetenz im Alltag der Schüler/innen, Lehrer/innen und Eltern immer mehr an Bedeutung.

Viele Lehrer/innen stellen sich die Frage, wie man den Umgang mit dem Internet für Kinder sicherer gestalten kann, denn sie tragen einen wesentlichen Teil dazu bei, den Schüler/innen nicht nur die Möglichkeiten sondern auch die Risiken des Internets und dessen Nutzung aufzuzeigen.

Es beschränken sich die Risiken nicht nur auf bedenkliche Inhalte im World Wide Web, wie z. B. Pornografie, Gewaltverherrlichung, Links- und Rechtsradikalismus, verstörende Inhalte, usw.. Die Nutzer von Onlinediensten sind auch noch mit vielen anderen Gefahren konfrontiert, wobei sich das Problem nicht nur auf Computernutzer beschränkt, sondern auch auf die Dienste für Mobiltelefone, die ebenfalls auf das Internet zugreifen können.

Zu diesen zählen unter anderem: Umgang mit persönlichen Daten, Angriffe aus dem Netz, Online-Betrug, mögliche Urheberrechtsverletzungen, Risiken bei der Kommunikation im Internet, Suchtgefahr-Internet, Meinungsmanipulation, usw..

Angesichts dieser unterschiedlichen Gefährdungen durch die Nutzung des Internets kann der Schutz vor diesen Risiken nicht alleine auf die Benutzung von Filterprogrammen reduziert werden, die außerdem bei weitem keinen lückenlosen Schutz vor jugendgefährdenden Inhalten des World Wide Web gewährleisten. Aus pädagogischer Sicht ist es daher unerlässlich, die Kinder zum kritischen und sicheren Umgang mit den neuen Medien zu führen. Gefragt ist also Medienkompetenz und nicht Einschränkung und Zensur.

2. Mögliche Gefahren im Internet

Inhalte

- Gewalt und Gewaltverherrlichung, auch in scheinbar harmlosen Online-Spielen
- Pornografische Inhalte
- Rechts- und linksradikale Seiten
- Rassismus
- Verstörende Inhalte (z. B. Freitodforen, Pro-Anorexie-Seiten, jugendschutzrelevantes Bild- und Filmmaterial,...)
- Sekten

Weitergabe von persönlichen Daten

- Namen, Adressen, Telefonnummern, E-Mail-Adressen, Fotos, z. B. in Foren oder Chatrooms
- Übertragung von Passwörtern durch ungesicherte Verbindungen (z.B. WLAN, http-Verbindungen)
- Eingabe von Kreditkartennummern, PINs, TANs in ungesicherten Umgebungen

Schutz vor Angriffen aus dem Netz

- Viren: Schadprogramme, die sich selbst verbreiten und Schaden anrichten können
- Spam-Mails: Unerwünschte, elektronisch übertragene Nachrichten, welche unverlangt zugestellt und massenhaft versandt werden
- Hacking: Unerlaubtes Eindringen in fremde Computer, um die Kontrolle zu übernehmen
- Phishing: Versuche, über gefälschte Internetadressen an Daten eines Internetnutzers zu gelangen
- Dialer: Computerprogramme, die über das Telefon/Handy kostenpflichtige Nummern anwählen und unbemerkt finanziellen Schaden anrichten
- Spyware und Trojaner: Programme, die ohne Wissen des Anwenders im Hintergrund laufen und z.B. persönliche Daten weitergeben
- Social Phishing: Ausforschen von wirtschaftlich relevanten persönlichen Daten und Verhaltensweisen

Umgang mit E-commerce (Online Shopping, Auktionen...):

- Unvorsichtiges und bedenkenloses Verhalten in Online-Shops, bei Online-Auktionen und Online-Gewinnspielen.

Urheberrechtsverletzungen

- Downloads und Verwendung von urheberrechtlich geschützten Inhalten
- Uploads und Veröffentlichung von urheberrechtlich geschützten Inhalten
- Tauschbörsen: Anbieten und Austauschen von urheberrechtlich geschützten Daten (zumeist Musik und Filme)
- Verwendung geschützter Fotos, Musik, Videos und Texten im Internet

Kommunikation im Internet

- Foren: Vermittlung von bedenklichen, verstörenden Inhalten
- Chats: Gefahr des Missbrauchs von Kindern und Jugendlichen durch Erwachsene
- Blogs: Wie bei Foren Konfrontation mit verstörenden Inhalten
- E-Mails: Sensible Inhalte sind grundsätzlich im Mail-Verkehr ungeschützt

Suchtgefahr Internet

- Realitätsverlust
- Soziale Isolation

Meinungsmanipulation

3. Medienkompetenz

Die Lebenswelt von Kindern und Jugendlichen wird genauso wie alle Teile der Gesellschaft von den Informationsmedien geprägt. Kommunikationsmedien sorgen für den raschen Austausch von Informationen, Bildern und Erkenntnissen, die durchaus auch zweifelhaften Inhalts sein können.

Die Fülle der Gefahren, die bei der Nutzung der Dienste des Internets auftreten, ist nicht nur auf die Inhalte des World Wide Webs beschränkt. Nur diese könnten aber durch den Einsatz technischer Hilfsmittel wie Filtersoftware zu einem geringen Teil abgemildert werden. Somit ist es aus medienpädagogischer Sicht nicht zielführend, bewahrungspädagogische Wege einzuschlagen, um den Gefahren aus dem Weg zu gehen.

Filtersoftware und andere Zensurmaßnahmen können zwar leicht im Wiener Bildungsnetz angewendet werden, führen aber eher dazu, dass auch viele andere pädagogisch wertvolle Inhalte im Internet nicht mehr erreichbar sind. Noch dazu würde diese Maßnahme die Benutzer (Schüler/innen und Lehrer/innen) in einer nur scheinbaren Sicherheit wiegen, denn ein hundertprozentiger Schutz ist auch hier nicht gegeben.

Pädagogisch ist es sicherlich sinnvoll, die Schüler/innen nicht nur auf einen Umgang mit den Neuen Medien im gesicherten Raum Schule vorzubereiten, sondern auch auf reale Gegebenheiten außerhalb dieses Schutzbereiches.

Eine pädagogische Zielsetzung kann daher nur sein, den Schüler/innen eine umfangreiche, kritische und sichere Haltung gegenüber den Gegebenheiten im Netz zu vermitteln. Sie also zu kompetenten und sicheren Nutzern zu machen, die über die Gefahren Bescheid wissen und diesen auch begegnen können, ohne Schaden zu nehmen oder anzurichten.

Wichtig ist es, den Stellenwert von Medien und Informationstechnologien für Kinder und Jugendliche in sensibler Weise zu erfassen und als Voraussetzung des Lernens mit und über Medien und Informationstechnologien zu berücksichtigen und Medien und Informationstechnologien angemessen zu handhaben.

Da mittlerweile ein Großteil der Schüler/innen auch im außerschulischen Bereich das Internet nutzt, kann Medienkompetenz nur in Zusammenarbeit mit den Eltern erreicht werden.

4. Tipps für einen kindgerechten Umgang mit dem Internet

Sowohl im schulischen als auch im privaten Bereich ist es unerlässlich, Absprachen zu treffen und Regeln für einen sicheren Umgang mit den Neuen Medien zu erstellen. Die Beachtung folgender Punkte soll den Lehrer/innen helfen, mögliche Gefahren rechtzeitig zu erkennen und Schaden abzuwehren.

Eine möglichst genaue Vorbereitung der Unterrichtseinheiten ist jedenfalls unerlässlich und schützt vor unliebsamen Überraschungen.

- Der Erwerb von grundlegenden Internetkenntnissen für den/die Lehrer/in, um mögliche Gefahren besser einschätzen zu können ist unerlässlich!
- Der Einsatz des Internets ist auf das Alter der Schüler/innen abzustimmen.
- Als Startseite soll im Webbrowser eine dem Alter der Kinder entsprechende Ausgangsplattform (z.B. www.kidsweb.at) voreingestellt sein, damit die Kinder vorerst im sicheren Bereich surfen.
- Bei Internetrecherchen oder Internetrallyes sollen altersadäquate sowie kindgerechte Suchmaschinen, wie z.B. www.blinde-kuh.de, www.milkmoon.de, www.trampeltier.de, verwendet werden.
- Altersgemäße Vereinbarungen (Regeln) zur Internetnutzung der Schüler/innen in der Schule sind zu treffen. Dabei sollen alle Beteiligten (Lehrer/innen, Schüler/innen und eventuell auch Eltern) in den Prozess der Erstellung sowie der Umsetzung der Vereinbarungen eingebunden sein.
- Schüler/innen sollen darauf aufmerksam gemacht werden, dass die Weitergabe von persönlichen Daten bei der Internetnutzung in der Schule nur nach Rücksprache mit dem/der zuständigen Lehrer/in erfolgen darf.
- Der Wahrheitsgehalt von Internetinhalten soll mit den Schüler/innen diskutiert und kritisch hinterfragt werden.
- Illegale Internetinhalte können an www.stopline.at gemeldet werden.

5. Vorschlag für Vereinbarungen, die mit den Schüler/innen getroffen werden können:

Bescheid sagen:

- Die Schüler/innen dürfen sich nicht ungefragt mit dem Internet verbinden. Sie müssen die/den zuständige/n Lehrer/in informieren, wenn sie ins Netz gehen. **Somit ist ein unbeaufsichtigtes Surfen im Internet, wie z.B. in Pausen, Freizeitstunden, usw. nicht möglich.**

Erlaubte Reiseziele:

- Die Schüler/innen surfen nur auf bekannten Internetseiten, über die Sie sich im Vorfeld gemeinsam mit den Schüler/innen informiert haben.

Neues nur gemeinsam:

- Neue Internetangebote werden zunächst nur gemeinsam angesehen.

Erste Hilfe:

- Sollte sich trotzdem eine Internetseite öffnen, die die Schüler/innen verwirrt oder ängstigt, schließen Sie den Browser und sprechen Sie mit ihnen darüber. Die Tastenkombinationen Strg+W schließt das Fenster bei den meisten Browsern.

Geheimsache persönliche Daten:

- Schüler/innen verraten im Internet – sei es in Chats, Foren oder E-Mails – ohne Rücksprache mit dem/der Lehrer/in niemals ihren Namen, ihre Klasse oder ihre Schuladresse.

Unbekannte sind Fremde – auch im Netz:

- Leute, die man im Internet "trifft", sind grundsätzlich Fremde und werden auch so behandelt. Egal wie nett sich Menschen geben, die Schüler/innen verraten nicht zu viel von sich und glauben nicht alles, was ihnen erzählt wird.

Nicht alleine registrieren:

- Wenn Internetangebote eine Anmeldung erfordern, informieren die Schüler/innen den/die zuständige/n Lehrer/in. Der/die Lehrer/in entscheidet dann ob eine Registrierung durchgeführt wird oder nicht.

Kein Einkaufsbummel ohne Zustimmung des/der Erziehungsberechtigten:

- Schüler/innen sind noch nicht geschäftsfähig und dürfen nicht eigenmächtig Bestellungen über das Internet aufgeben. Daher ist bei der Internetnutzung in der Schule ein solcher „Einkaufsbummel“ zu untersagen.

6. Mögliche Maßnahmen im Wiener Bildungsnetz (WBN) bei wiederholten bewussten Verstößen gegen die getroffenen Vereinbarungen

Diese Maßnahmen sind vom/von der zuständigen IT-Kustoden/Kustodin durchzuführen und bei Bedarf im Vorfeld im Lehrer/innenkollegium zu besprechen.

- Ausblendung der Adressenleiste im Internetexplorer → Schüler/innen können auf dem betreffenden PC keine Internetadressen mehr eingeben.
- Aktivierung vom Inhaltsratgeber des Internetexplorers → Schüler/innen können auf dem betreffenden PC nur mehr jene Internetseiten aufrufen, die durch die Lehrer/innen explizit freigegeben wurden.
- Deinstallierung des Internetexplorers auf einzelnen Computern → Keine Einstiegsmöglichkeit mehr ins WWW für Schüler/innen auf dem betreffenden PC.
- Sperre des pädagogischen Internetzuganges für die ganze Schule → (HS/KMS, ASO und PTS - einzelne Lehrsäle, Volksschulen – für alle Klassen).

7. Linkempfehlungen

Suchmaschinen für Kinder

www.blinde-kuh.de
www.milkmoon.de
www.trampeltier.de
www.helles-koepfchen.de
www.kindercampus.de/clikks
www.cyberzwerge.de
www.kindernetz.de/suche
www.spielstrasse.de/fs_search.htm

Kindgerechte Seiten

www.kidsweb.at
www.kidsnet.at
www.kidsweb.de
www.toggolino.de
www.geo.de/GEOlino
www.seitenstark.de

Links zum Thema „Sicheres Internet“

www.saferinternet.at
www.sicher-im-internet.at
www.internet-abc.de
www.klicksafe.de
www.stopline.at
www.mpfs.de/fileadmin/Infoset/Internet-DownloadHP.pdf
www.bsi-fuer-buerger.de
www.internauten.de