1 Medienpädagogik - Durch pädagogisches Herangehen den Umgang mit neuen Medien sicherer gestalten!

Kinder und Jugendliche nutzen heutzutage völlig selbstverständlich eine Vielzahl moderner Medien. Dabei sind die Heranwachsenden unserem eigenen Wissen über Internet, Social Networks, Chat Clients, usw. in Sachen Bedienung und Nutzung oftmals sehr weit voraus. Dennoch ist es erforderlich, dass wir sie auf ihrem Weg begleiten und beschützen, denn nicht alle Gefahren können von Kindern und Jugendlichen richtig abgeschätzt oder überhaupt erkannt werden. In diesem Merkblatt werden die wichtigsten Gefährdungen vorgestellt, damit Sie in der Familie einen eigenen Umgang mit dieser Problematik finden können.

2 Kommunikation vs. Datenschutz

Im Internet können Informationen mit vielen Menschen geteilt werden. Wer mitteilen will, welchen Song er gerade liebt, wie der Schulalltag war oder welchen Hobbys er wie erfolgreich nachgeht, hat in Social Networks, Foren und Chatclients verschiedener Anbieter eine breite Palette von Tools an der Hand. Es wird propagiert, dass der Nutzen dieser Medien umso größer ist, je mehr an Informationen man über sich Preis gibt – hat man so doch bspw. die Möglichkeit, neue Freunde mit ähnlichen Interessen zu gewinnen. Man sollte sich dabei aber einiger Umstände bewusst sein:

3 Wer soll was mit den Daten Ihrer Kinder anstellen dürfen?

Die Anbieter der verschiedenen Kommunikationskanäle handeln aus wirtschaftlichen Interessen heraus. Eine Geschäftsgrundlage ist dabei das Sammeln von Daten, um bspw. personalisierte Werbung einzublenden. Auch die Weitergabe der Daten an Dritte ist nicht ausgeschlossen. Es gilt daher, die Nutzungsbestimmungen nicht einfach bei der Anmeldung eines der Dienste wegzuklicken, sondern sich diese durchzulesen, um eine Vorstellung davon zu gewinnen, wer alles was mit den eigenen Daten anstellen könnte. Da Kinder und Jugendliche hierbei wegen des „Vertragsdeutsch“ Schwierigkeiten haben dürften, sollte die Vereinbarung getroffen werden, dass die Eltern hierbei helfend zur Seite stehen. Wichtig ist in diesem Zusammenhang auch, dass die Nutzungsbestimmungen teilweise mehr oder weniger stillschweigend von den Anbietern geändert werden. Es bedarf also regelmäßiger Kontrolle der möglichen Änderungen.

4 Sind Ihre Kinder vorsichtig genug, nur Daten einzustellen, die ihnen später nicht zum Nachteil gereichen können?

Die Daten, die ins Netz gestellt werden, können für nahezu unbegrenzte Zeit gespeichert werden. Einmal eingestellte Daten sind nur unter großen Schwierigkeiten wieder zu löschen. Es gilt daher zu überlegen, ob die Daten später einmal zum Nachteil gereichen können. Wer im Netz damit prahlt, ständig die Nacht zum Tag zu machen und andere beim Feiern in Sachen Alkoholkonsum zu übertrumpfen, darf sich nicht wundern, im Vorstellungsgespräch besonders kritisch beäugt oder überhaupt nicht eingeladen zu werden. Als Faustregel sollte man sich daher fragen, ob man möchte, dass auch in 10 Jahren noch jeder wissen darf, was man gerade jemandem online mitteilen möchte. Kinder werden hier im Regelfall größere Schwierigkeiten bei der Abschätzung haben, andererseits werden die geäußerten Interessen auch harmloser ausfallen.

5 Teilen sich Ihre Kinder nur Freunden oder der „halben Welt“ mit?

Auf die Datenschutzbedürfnisse der Kunden wird von Seiten der Social Network-Anbieter bisweilen schon eingegangen. Es gibt Möglichkeiten, die Reichweite der Weitergabe von privaten Informationen einzuschränken. Hier sollten Sie mit ihrem Kind zusammen die Einstellungen durchgehen und darauf achten, dass nach Möglichkeiten nur „Freunde“, also vom Nutzer bestätigte Kontakte, die Mitteilungen lesen können. Bei manchen Netzwerken gibt es die Voreinstellung, dass nur Freunde von Freunden Nachrichten lesen können. Da aber in Social Networks oft große Anzahlen von virtuellen Bekanntschaften geschlossen werden, kommen so schnell unüberschaubare Mengen an Mitlesern zusammen. Ein Durchschnittsuser von Facebook soll etwa 150 Kontakte haben – mitlesen können bei der genannten Einstellung also rund 150 x 150 = 22500 Menschen, also die Dimension einer Kleinstadtbevölkerung. Auch hier gilt, dass die Einstellungen vom Hersteller wieder zurückgesetzt werden können – man muss also regelmäßig überprüfen, ob sich hier etwas geändert hat.

6 Cyberkriminalität – Abo-Fallen und andere unerwünschte Verträge

Wie im gesellschaftlichen Leben insgesamt, gibt es auch im Netz nicht nur weiße Schafe. Es existieren mehrere Möglichkeiten, ins Ziel von kriminellen Absichten zu geraten. Bei Erwachsenen sind die Dimensionen wirtschaftlicher Verluste zwar deutlich höher, dennoch gibt es auch Fallen, in die Heranwachsende tappen können. So gibt es z.B. Werbebanner, die mit vermeintlichen Gewinnaussichten versuchen, Menschen zu Abschlüssen von Verträgen zu bewegen. Hier sollte man keinesfalls seine persönlichen Daten eingeben. Zumindest gilt es, das Kleingedruckte auch zur Kenntnis zu nehmen. Da hier nicht immer rechtskonform gearbeitet wird, kann es sein, dass überhaupt nicht ersichtlich wird, dass durch das Ausfüllen eines Formulars ein Kauf- oder Dienstleistungsvertrag geschlossen wird. Im Schadensfall kann hier nur noch die Verbraucherzentrale weiterhelfen. Kindern sollte also klargemacht werden, dass Geschenke im virtuellen Raum wie im regulären Leben eine Ausnahme sind und sie sich – falls die Verlockung doch zu groß ist – an ihre Eltern wenden sollen.

7 Den eigenen PC, das eigene Handy absichern

Auch der eigene Computer, das eigene Handy kann das Ziel krimineller Absichten sein. Viren und Trojaner werden dazu benutzt, die Fernsteuerung des eigenen PC durch Kriminelle zu ermöglichen. So dient er in Zukunft zum Versand von Werbemails (Spam), als Teil eines sogenannten Botnetzes Angriffen auf fremde Rechnerstrukturen oder es werden persönliche Daten ausgelesen (bspw. Kreditkarteninformationen). Hiervor kann man seinen Rechner nur begrenzt schützen. Es hilft, dem eigenen Betriebssystem zu erlauben, sich regelmäßig mit Sicherheitsupdates zu versorgen und einen Virenschutz zu installieren. Auch andere Programme sollten regelmäßig aktualisiert werden, vor allem der Internetbrowser. Programme sollten nur von vertrauenswürdigen Seiten heruntergeladen werden und Seiten, die Raubkopien verbreiten, sind ein besonders hohes Infektionsrisiko für den eigenen PC. Da Kindern die Unterscheidung zwischen sicheren und unsicheren Quellen nur schwer möglich sein dürfte, sollte überlegt werden, Kindern einen eigenen Benutzer-Account mit eingeschränkten Rechten zuzuweisen.
Beim Mailverkehr gilt: grundsätzlich keine Anhänge von Mails unbekannter Absender öffnen, diese sehr genau prüfen und im Zweifelsfall löschen.
Bezahlen im Internet ist am Sichersten mit Prepaid-Kreditkarten, die es inzwischen überall gibt.
Auch die Passwortsicherheit trägt zum Schutz eigener Daten bei. Es sollten mehrere Passwörter nebeneinander und nur zeitlich befristet verwendet werden. Sichere Passwörter enthalten Groß- und Kleinbuchstaben, sowie Zahlen und Sonderzeichen und insgesamt mindestens acht Stellen. Sie dürfen nach Möglichkeit keinen Sinn ergeben, also nicht erraten werden können.

8 Filesharing und Abmahnungen als Folge

Daneben sollte Kindern und Jugendlichen natürlich klar gemacht werden, dass es auch im Internet Rechtsverstöße gibt, die Anzeigen und Abmahnungen zur Folge haben können. Insbesondere, aber nicht ausschließlich, gilt das für sogenannte Tauschbörsen (Filesharing-Tools). Hier werden die herunter geladenen Dateien meist automatisch anderen Nutzern zur Verfügung gestellt, sodass man aus Sicht der Rechtsprechung nicht nur für die illegale Aneignung urheberrechtlich geschützten Materials haftbar ist, sondern auch für die Verbreitung desselben. Hieraus leitet die betroffene Unterhaltungsindustrie hohe Schadensersatzsummen für sich ab und entsprechende Abmahnungen können empfindlich teuer werden. Es empfiehlt sich evtl., die Nutzung von Tauschbörsen etc. generell zu untersagen.

9 Cybergrooming – Auch Pädophile nutzen das Internet

Die Achtsamkeit im Umgang mit eigenen Daten wird noch wichtiger vor dem Hintergrund des leider vorhandenen Phänomens des Cybergroomings. Pädophile nutzen die Anonymität des Internets aus, um ohne die Gefahr sozialer Kontrolle durch Mitbürger gefahrlos Kontakt zu Kindern und Jugendlichen herzustellen. Da die Identität von Chatpartnern nicht ohne weiteres festzustellen ist, geben sich Pädophile als Gleichaltrige aus und erschleichen so langsam das Vertrauen potentieller Opfer. Kinder und Jugendliche müssen daher ein Bewusstsein von der Möglichkeit der Identitätsverschleierung haben. Am besten werden Freundschafts- oder Chateinladungen im virtuellen Raum nur nach vorheriger Vereinbarung im realen Leben verschickt oder angenommen. Wenn Kindern oder Jugendlichen etwas unangenehm im Chat ist, müssen sie sich vertrauensvoll an ihre Eltern wenden können. Das sollte ihnen unmissverständlich klar gemacht werden. In durch Administratoren betreuten Netzwerken wie SchülerVZ gibt es zudem die Möglichkeit, Personen zu melden, die sich in unangebrachter Weise verhalten haben. So können weitere Personen geschützt werden, indem der User nach Überprüfung durch die Administratoren

aus dem Netzwerk verbannt wird. Kinder und Jugendliche sollten sich niemals ohne erwachsene Begleitpersonen mit virtuellen Freunden treffen oder im Chat Angaben machen, die auf eine Identifikation schließen lassen (Schule, Nach-Hause-Weg, Wohnhaus, etc.). Wo immer möglich sollte daher auch auf den Realnamen verzichtet werden, insbesondere beim Chatten empfiehlt sich ein Spitzname (Nickname). Auch ist es besser, kein die eigene Person erkenntlich machendes Profilbild zu verwenden, die eigene Identität nicht preiszugeben.

10 Rechte anderer & Cyber-Mobbing

So viel Spaß es auch macht, Fotos von interessanten Ereignissen mit Freunden zu teilen, es muss klar sein, dass es Persönlichkeitsrechte wie das Recht am eigenen Bild gibt. Das gilt in beide Richtungen: Man muss es sich nicht gefallen lassen, dass andere Nutzer von sozialen Netzen ungefragt Bilder oder Klatsch über die eigene Person ins Netz stellen - hier kann man auf Löschung bestehen und dazu ggf. auch einen Administrator der Seite anschreiben. Man sollte aber auch selbst die Rechte anderer respektieren und vor dem Posten beteiligte/betroffene Personen um Erlaubnis fragen. Das gilt erst recht für beleidigende oder demütigende Inhalte. Diese haben so wenig im Netz verloren wie auf dem Schulhof oder im Klassenzimmer. Falls Kinder sich ihren Eltern nicht anvertrauen möchten, können sie auch kostenlos bei der „Nummer gegen Kummer“ (0800 111 0 333) anrufen (die Berater sind generell mit kinder- und jugendspezifischen Problemen vertraut).

11 Unerwünschte Inhalte herausfiltern

Es ist sehr schwierig, Heranwachsende wirkungsvoll vor unerwünschten Inhalten wie gewalttätigen Videos, pornographischem Material oder politischem Extremismus im Internet zu schützen. Solange Kinder nur einzelne Seiten nutzen können sollen, empfehlen sich sogenannte White-List-Filter. Hier wird jede einzelne kindesgemäße Seite einzeln freigeschaltet, alles andere kann nicht angesurft werden. Je größer der Wissensdrang wird, umso schwieriger wird es allerdings, einen sinnvollen virtuellen Spielraum abzustecken. Daher existieren Filterprogramme (teils kostenlos, teils kostenpflichtig), die den Anspruch erheben, sämtliche Seiten im Internet daraufhin zu beurteilen, ob sie jugendgefährdend sind. Die Praxis zeigt jedoch, dass diese Systeme es nicht fehlerfrei schaffen, das Internet in dieser Hinsicht zu kontrollieren. Auch sind diese Tools manchmal übereifrig und blockieren aus wenig nachvollziehbaren Gründen einzelne Webanbieter. Zudem lassen sich die Systeme teilweise relativ leicht durch technisch versierte Jugendliche aushebeln. Der Einsatz solcher Software ersetzt daher nicht die elterliche Kontrolle ihrer Kinder.

12 Fazit

Aus dem Bisherigen sollte deutlich geworden sein, dass es genauso wichtig ist, Kinder- und Jugendliche auf ihrem Weg in die virtuelle Welt zu begleiten wie im realen Leben. Die Entscheidungen, die mit der Freiheit des Internets auf die Nutzer zukommen, sind selbst für viele Erwachsene nicht leicht zu treffen. Daher sollten die virtuellen Freiheiten des Kindes im Umgang mit der Mediennutzung wie auch die im realen Leben schrittweise und der individuellen Entwicklung gemäß angepasst werden. Fahrlässig wäre sowohl Gleichgültigkeit angesichts der vielen Risiken (beispielsweise der eigene internetfähige PC im Kinderzimmer eines Grundschulkindes), wie auch eine totale Verweigerungshaltung. Denn für Berufsanfänger wird ein selbstverständlicher Umgang mit modernen Medien oftmals bereits unterstellt. Es ist daher eine wichtige Erziehungsaufgabe, sinnvolle Regeln innerhalb der Familie zu erarbeiten und deren Einhaltung zu überwachen. Eine erste Orientierung wurde in diesem Merkblatt geliefert. Weitere Informationen können u.a. unter folgenden Internetadressen bezogen werden:

Für Eltern und Pädagogen:

https://www.klicksafe.de/materialien/index.html
http://www.jugendschutz.net/
http://www.bmelv.de/cln_154/DE/Verbraucherschutz/Telekommunikation/Internet/Internet_node.html

Für Schüler:
http://www.klick-tipps.net/ http://www.blinde-kuh.de/