

Datenschutz TIPPS

für Eltern



▶ So sind persönliche
Daten im Internet sicher



klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

Datenschutz TIPPS

für Eltern

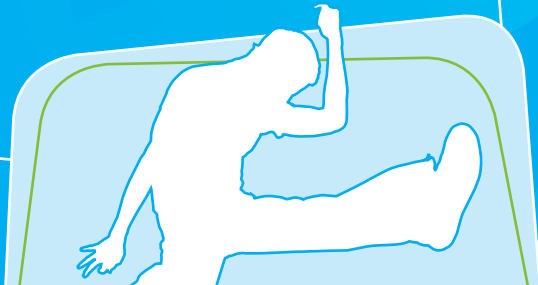
Liebe Eltern!

Viele Jugendliche glauben, Datenschutz sei langweilig und gehe sie nichts an. Überzeugen Sie Ihr Kind vom Gegenteil! Wenn Sie oder Ihr Kind das Internet nutzen, dann lesen Sie unsere folgenden Tipps.

Denn jeder Internet-Nutzer hinterlässt Spuren im Netz – immer. Sobald man im Internet unterwegs ist, werden Daten über das eigene Surfverhalten gesammelt. Manche verraten die Nutzer selber, bei anderen ist es dem Nutzer oft gar nicht bewusst, dass sie gesammelt werden.

Wir sagen Ihnen, was Sie für den Schutz von persönlichen Daten im Internet tun können.

Ihr Klicksafe-Team



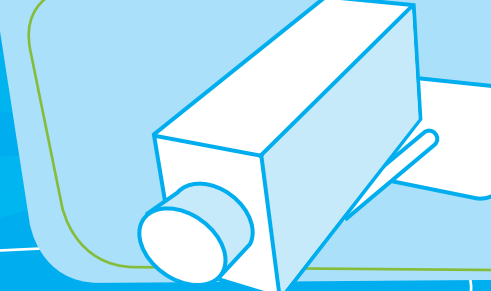
1

Datenschutz geht uns alle an

► Datenschutz – das klingt für Kinder und Jugendliche zunächst ziemlich trocken, kann Ihrem Kind aber Ärger ersparen und helfen, sich im Internet frei zu bewegen. Denn viele Informationen sind eher privat und gehen andere Personen nichts an. Auch Ihre Kinder sollten sich um den Schutz Ihrer Daten kümmern!

Alle Daten, die etwas mit der eigenen Person zu tun haben, zum Beispiel Adresse, Alter oder Interessen, sind „**personenbezogene Daten**“. Sie verraten viel über die eigene Person und sind kostbar. Für Unternehmen bedeuten sie bares Geld, und sie können von anderen missbraucht werden. Schützt man seine Daten, heißt das Privatsphäre, Anonymität und mehr Sicherheit im Internet! Dies sollte auch jüngeren Internetnutzern klar sein!

- ⊕ Die schöne neue Welt der Überwachung www.panopti.com.onreact.com
- ⊕ Bildergeschichte Datenschutz
www.handysektor.de/index.php/bildergeschichten/datenschutz/



2

Datenschutz ist ihr gutes Recht

► Durch das „**Recht auf informationelle Selbstbestimmung**“ sind persönliche Daten (wie Name, Adresse, Telefonnummer) in Deutschland sogar per Gesetz vor unerlaubter Verwendung geschützt. Das bedeutet: Niemand darf diese Daten ohne Einwilligung der betroffenen Person speichern, veröffentlichen oder weitergeben. Ausnahmen gibt es für einige staatliche Einrichtungen, wie zum Beispiel Meldeämter oder die Polizei.

Was aber gilt für Fotos und Filme? Hier gibt es das „**Recht am eigenen Bild**“: Ausschließlich die abgebildete Person darf entscheiden, welche Bilder von ihr veröffentlicht werden dürfen. Das gilt sogar für Fotos, auf denen das Gesicht verfremdet wurde, die Person aber durch andere Merkmale (wie die Körperhaltung oder eine Tätowierung) eindeutig zu erkennen ist. Ausnahmen gelten für Bilder, auf denen man Teil einer Menschenmenge oder nur „Beiwerk“ ist (Beispiel: Jemand fotografiert den Reichstag und Sie oder Ihr Kind stehen zufällig daneben). Im Internet können Sie von den Betreibern eines Webangebotes schriftlich die Löschung der persönlichen Daten eines noch nicht volljährigen Familienmitglieds verlangen, zum Beispiel das Profil Ihres Kindes in einem sozialen Netzwerk wie Facebook oder SchülerVZ mit sämtlichen Bildern und Texten.

Übrigens: Wenn Ihr Kind jünger als 18 Jahre alt ist, haben Sie als Eltern bzw. Erziehungsberechtigte bei Veröffentlichungen mitzuentcheiden. Ist Ihr Kind jünger als 14 Jahre, muss Ihr Kind Sie in jedem Fall um Erlaubnis fragen!

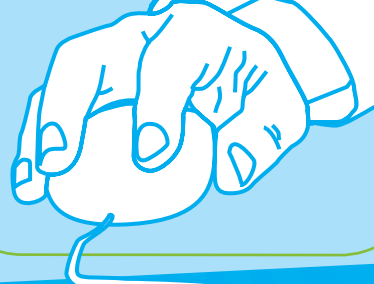
- 🌐 Checked4you – Deine Rechte im Web (Klicken Sie auf Computer + Internet, dann auf Internet) www.checked4you.de

3

Jeder hat ein Recht auf Datenschutz

► Ihr Kind sollte nicht nur die eigenen, sondern auch die Persönlichkeitsrechte anderer wahren. Denn: Jeder hat ein Recht am eigenen Wort und am eigenen Bild. Machen Sie Ihrem Kind klar, dass es keine Bilder, Filme und Infos von anderen ins Netz stellt, es sei denn, es hat die Erlaubnis. Generell ist es verboten, falsche Daten über jemanden zu veröffentlichen. Das wäre Rufschädigung und kann sogar bestraft werden. Tipp: Ihr Kind soll sich vorab überlegen, ob es selbst mit der Veröffentlichung entsprechender Fotos, Filme oder Infos einverstanden wäre. Falls nicht, dann sollte man von einer Veröffentlichung absehen! Das ist ein Zeichen von **Respekt**. Ihr Kind soll nicht die Rechte anderer verletzen – egal ob im Internet oder in der wirklichen Welt.

- 🌐 Unter www.irights.info finden Sie weitere Infos zum Thema „Urheberrecht in der digitalen Welt“
- 🌐 Auf www.chatiquette.de werden Tipps und Benimmregeln fürs Chatten vorgestellt



4 So wird ihr Kind ein Datenprofi in sozialen Netzwerken

► Für den Schutz der eigenen Privatsphäre ist Ihr Kind auch selbst verantwortlich. Es sollte darauf achten, wie es sich im Netz zeigt! Geben Sie Ihrem Kind die folgenden Tipps mit auf den Weg:

- **Peinliche** Fotos, Filme und **persönliche** Infos haben im Netz nichts zu suchen. Sie verraten viel über die eigene Person, können später den Ausbildungsplatz kosten und generell Ärger bringen. Arbeitgeber durchforsten heute das Internet, um Bewerber zu überprüfen.
- Auch **Gruppenmitgliedschaften** teilen anderen viel von dir mit. Verzichte auf Gruppen wie „Saufen bis der Arzt kommt“, etc. Diese sind nicht die beste Werbung für dich. Hassgruppen, in denen andere gezielt beleidigt werden, sollten in jedem Fall gemieden werden.
- Sei sorgsam mit deinen **Profil-Daten**: Lass Anschrift, Telefon- oder ICQ-Nummern (ICQ ist ein Programm zum Nachrichtenaustausch in Echtzeit) weg. Sie sind nicht nötig, wenn du dich innerhalb der Community austauschst. Auch deine private E-Mail-Adresse solltest du nicht jedem geben.
- Setz deine **Profileinstellungen** auf privat. Nur Freunde sollten die Angaben sehen.
- Prüfe auch, ob du all deine „**Online-Freunde**“ wirklich gut genug kennst, um ihnen freien Zugang zu deinen privaten Fotos und Daten zu geben. Du weißt nie, was sie mit den Informationen machen!

Das heißt aber nicht, dass Ihr Kind ganz auf persönliche Informationen verzichten muss. Entscheidend ist die Auswahl der richtigen Infos. Überlegen Sie sich einmal gemeinsam mit Ihrem Kind: Welche Daten möchte ich der Welt auf ewig präsentieren?

Wenn Ihr Kind ein soziales Netzwerk nicht mehr nutzen will, dann sollte es seine Mitgliedschaft beenden und die Profildaten löschen.

So wird das Auffinden persönlicher Daten zumindest erschwert.

- ⊕ So schützt Ihr Kind seine persönlichen Daten in verschiedenen sozialen Netzwerken (Klicken Sie oben auf Materialien, dann auf klicksafe-Leitfäden für Soziale Netzwerke und Instant Messenger): www.klicksafe.de
- ⊕ Zum Schutz vor Missbrauch kann Ihr Kind auch das eigene Profilfoto witzig verändern, sodass man nicht zu erkennen ist. (Klicken Sie auf Workshops, dann auf Profilbilder und Icons): www.netzcheckers.de
- ⊕ Tipps für mehr Privatsphäre in schüler- und studIVZ zum Download: „Big brother is watching you!“ www.jugendinfo.de/pass-auf-dich-auf

5 Das Internet vergisst nicht

► Reden Sie mit Ihrem Kind darüber, dass persönliche Infos, Texte, Filme und Fotos, die ins Internet gestellt werden, ab da nicht mehr privat sind. Einmal im Internet, beginnen diese Daten ein **Eigenleben**. Sie verbreiten sich, gelangen in Suchmaschinen und Online-Archive, werden von anderen Nutzern kopiert und weitergereicht. Dies alles wieder rückgängig zu machen, ist nahezu unmöglich. Daher gilt: Vorher überlegen, was wirklich alle von einem wissen dürfen!

- ⊕ Das Internet-Archiv „WayBack Machine“ speichert Webseiten als Zeitdokumente dauerhaft ab www.archive.org
- ⊕ Videos Think Before You Post www.smiley-ev.de/think_before_you_post.php
- ⊕ Videos auf www.klicksafe.de/spots/index.html

6 Elektronische Daten-Spuren hinterlässt man unbemerkt

- Technische Daten werden automatisch übertragen, ohne dass man es merkt. Gerade dies ist Kindern und Jugendlichen häufig nicht klar. Zwei Beispiele:
- Jeder Computer, der sich ins Internet einloggt, erhält eine **IP Nummer** – eine Art „Telefonnummer für das Internet“. Damit lässt sich genau nachvollziehen, wann, wie lange und auf welchen Seiten der Nutzer im Netz unterwegs war. Über die IP-Nummer kann die Polizei bei Straftaten, wie zum Beispiel illegalen Musikdownloads, den Täter ermitteln.
- Das Kind surft auf der Seite seiner Lieblingsband und sieht kurze Zeit später auf einer anderen Seite eine Werbung für ihre neue CD. Wie kommt das? Schuld daran können **Cookies** („Kekse“) sein. Cookies sind kleine Datenpakete, die auf dem Rechner gespeichert werden und sich merken, welche Seiten besucht worden sind. So können Unternehmen den Internet-Surfer beobachten und herausfinden, welche Interessen er hat.

- ! Überprüfen Sie Ihre Browser-Einstellungen (Browser = Internetprogramm wie Internet Explorer und Firefox) und lassen Sie sich darüber anzeigen, wann eine Seite ein Cookie setzen will. So kann selbst entschieden werden! Die Einstellungen finden Sie unter:
Internet Explorer: Extras > Internetoptionen > Datenschutz > Erweitert
Firefox: Extras > Einstellungen > Datenschutz

7 Nicknames nutzen – unerkant surfen

- Ein guter **Nick** („Deckname“) kann dabei helfen, im Internet unerkant zu surfen. Hierbei ist Erfindungsgeist gefragt – ein Deckname, der dem richtigen Namen zu ähnlich ist oder das Alter enthält, hilft wenig. Ihr Kind kann ihn zum Beispiel in Blogs, Chats und Foren benutzen. Machen Sie Ihrem Kind auch klar, dass es sich nicht hinter einem Nick verstecken oder sich als jemand anderer ausgeben soll, um andere gezielt zu beleidigen. Das ist unfair und kann sogar bestraft werden! Auch wenn Ihr Kind in Netzwerken wie zum Beispiel schülerVZ gefunden werden will, sollte es hier zumindest den Nachnamen abkürzen und nicht voll ausschreiben.
- ! Je häufiger Ihr Kind das Internet aktiv nutzt, umso sicherer ist es, wenn es verschiedene Nicks verwendet. So bietet Ihr Kind weniger Angriffsfläche für Beleidigungen, Betrug und anderen Datenmissbrauch.



8

So behält ihr Kind die Kontrolle über seine Daten

► Je mehr Daten Ihr Kind im Internet von sich veröffentlicht, umso weniger können diese kontrolliert werden. Erklären Sie Ihrem Kind, dass es sich nicht selbst das Recht auf informationelle Selbstbestimmung nehmen sollte (siehe auch Punkt 2)! **Datensparsamkeit** lohnt sich und schützt vor bösen Überraschungen. Gemeinsam mit Ihrem Kind können Sie entscheiden, welche persönlichen Daten es ohne Probleme im Netz veröffentlichen darf. Fragen Sie Ihr Kind, ob es seine Daten (noch) im Griff hat!

Häufig ist es aber auch das Problem, dass andere Personen private Dateien, Informationen oder Fotos von Ihrem Kind veröffentlichen. Aus diesem Grunde sollten Sie den eigenen und den „Online-Ruf“ Ihres Kindes regelmäßig mit Suchmaschinen überprüfen und sich anschauen, wie man im Netz erscheint.

🌐 Personensuchmaschinen: www.yasni.de www.123people.de www.spock.com

9

Die AGBs – Was der Anbieter mit den Nutzerdaten machen darf

► Gerade Kindern und Jugendlichen fällt es häufig schwer, die **AGBs**, die Allgemeinen Geschäftsbedingungen eines Internet-Angebots, zu lesen und zu verstehen. Vor allem die hier enthaltene **Datenschutzerklärung** ist überaus wichtig und sollte genau studiert werden. Der Nutzer erfährt hier, was mit seinen Daten passiert, was gespeichert, weitergegeben oder für Werbung genutzt wird. Bevor Ihr Kind ein Web-Angebot nutzt, prüfen Sie genau, welche Angaben der Anbieter zum Datenschutz macht. Vereinbaren Sie mit Ihrem Kind, dass Sie neue Internetangebote vor einer Neuanmeldung gemeinsam anschauen und prüfen. Sagen Sie Ihrem Kind, dass es sich bei Fragen jederzeit an Sie wenden kann. Im Zweifel sollte Ihr Kind lieber auf eine Nutzung des Angebots verzichten – auch wenn es häufig schwerfällt.

Hier **zwei Beispiele** von vielen:

- Bei vielen **Instant Messengern** (Programme zum Nachrichtenaustausch in Echtzeit) gibt man allein durch die Nutzung sämtliche Rechte an allen versendeten Inhalten ab. Damit darf der Anbieter des Programms beispielsweise auch an Freunde verschickte Nachrichten speichern, bearbeiten und sogar veröffentlichen.
- Viele kostenlose **E-Mail-Anbieter** „lesen“ die Inhalte von E-Mails automatisch nach Schlüsselwörtern aus, um dem Nutzer dazu passende Werbung zu senden.

10

Andere machen sich ein genaues Bild von ihrem Kind

► Unternehmen wollen möglichst viel von Ihren Nutzern erfahren. Sie haben ein Interesse daran, die Klicks und Angaben, die man auf verschiedenen Seiten gemacht hat, miteinander zu verknüpfen. Alle Daten, die sich über eine Person im Internet finden lassen, können zu einem **Nutzerprofil** zusammengestellt werden. So können Unternehmen passende Werbung zeigen, oder die Nutzer mit Werbemails zuschütten. Denn je mehr man von einem Nutzer weiß, desto eher kann man ihn zielgenau umwerben. Diese **personalisierte Werbung** ist häufig so geschickt, dass man gar nicht merkt, wie man vom Kauf bestimmter Produkte überzeugt wird.

🌐 Infos und Tipps zum Thema Datenschutz im Internet: www.datenparty.de

11

Vor Datenmissbrauch ist niemand geschützt

► Persönliche Daten sind im Netz nie völlig sicher und können leicht in falsche Hände geraten. Es gibt Kriminelle im Internet (sogenannte Hacker), die Daten stehlen und auch Computerfehler und Datenpannen sind keine Seltenheit. Bei einem großen deutschen Schüler-Netzwerk wurden bereits rund eine Million Profildaten gehackt und illegal weitergegeben. Auch deshalb gilt für Ihr Kind: Überlege gut, was du ins Netz stellst.

Sollten Sie oder Ihr Kind von Datenschutzverletzungen wissen oder selbst betroffen sein, melden Sie diese und gehen dagegen vor! Als Beweis sollte man einen Screenshot („Foto“ vom Bildschirm) machen. Hierzu drücken Sie die Taste „Druck“ auf Ihrer Tastatur, fügen das Bild mit den Tasten „STRG“ + „V“ in ein Bildbearbeitungs- oder Schreibprogramm ein und speichern es ab.

- Wenn Sie wissen, wer die problematischen Infos oder Bilder im Internet veröffentlicht hat, sollten Sie zunächst diese Person bitten, die Inhalte so schnell wie möglich zu löschen. Geben Sie hier eine konkrete Frist an, bis zu der die Inhalte entfernt sein müssen.
- Wenn dies nichts bringt, informieren Sie den Betreiber der Seite und bitten um Löschung (Sie finden die Kontaktdaten im **Impressum** der Internetseite – gesetzlich vorgeschriebene Angabe über den Verantwortlichen für die Internetseite – oder über www.whois.net und www.denic.de). Erklären Sie Ihrem Kind, dass es sich jederzeit bei allen Problemen rund um das Internet an Sie wenden kann.
- Bei falschen Behauptungen oder Beleidigungen gegen Personen kann auch die **Polizei** eingeschaltet werden.
- Die **Datenschutz-Aufsichtsbehörden** der Bundesländer können Ihnen bei Datenschutzverletzungen ebenfalls mit Rat und Tat zur Seite stehen.
- Bei verbotenen oder jugendgefährdenden Inhalten (z. B. pornografische Bilder) sind die **Beschwerdestellen**, wie etwa www.jugendschutz.net oder www.internet-beschwerdestelle.de, der passende Ansprechpartner.

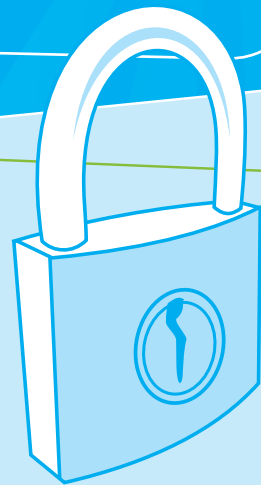
- 🌐 Die Adressen der Datenschutz-Aufsichtsbehörden der Länder finden Sie auf www.bfdi.bund.de (Klicken Sie auf Datenschutz + Anschriften und Links + Aufsichtsbehörden für den nicht-öffentlichen Bereich)
- 🌐 Virtuelles Datenschutzbüro www.datenschutz.de

12

Sicherheitstipps – So sind die Daten Ihrer Familie gesichert

- Folgende Sicherheitstipps helfen Ihnen und Ihrem Kind, wichtige Daten zu schützen:
- Benutzen Sie **sichere Passwörter** (mindestens 8-stellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen wie „+-\$%&“) und nicht immer das gleiche. Es sollten nicht der Name eines Haustieres, ein Spitzname oder ähnliche leicht zu erratende Wörter sein. Merksätze können dabei helfen, die Passwörter nicht zu vergessen. Erklären Sie Ihrem Kind, warum es Passwörter nicht weitergeben sollte. So wird verhindert, dass Fremde auf wichtige Daten zugreifen können.
- Installieren Sie ein **Anti-Virenprogramm** und aktualisieren Sie es regelmäßig
- Schützen Sie Ihren Computer mit einer **Firewall** („Brandwand“). Eine Firewall schützt vor Angriffen und unberechtigten Zugriffen aus dem Internet und sollte nie ausgeschaltet werden.
- Gehen Sie zu Hause kabellos ins Internet? Dann sollten Sie Ihr **WLAN-Netzwerk** über eine verschlüsselte Verbindung sichern. Von unterwegs sollte man beim kabellosen Surfen keine wichtigen Daten verschicken. Zudem sollte man das WLAN ausschalten, wenn es nicht benötigt wird.
- Führen Sie regelmäßig **Sicherheitsupdates** (Update=Aktualisierung) Ihres Betriebssystems durch. Am besten stellen Sie es so ein, dass Sie wichtige Updates automatisch erhalten. So werden Sicherheitslücken geschlossen.

- Sagen Sie Ihrem Kind, dass es keine E-Mails mit unbekanntem Absender öffnen sollte, vor allem keine mitgeschickten Dateien. Auch sollte es nicht auf unerwünschte E-Mails antworten. Weitere nervige Mails wären die Folge! Am besten legen Sie jedem Familienmitglied **zwei verschiedene E-Mail-Adressen** an. Eine sollte nur an gute Freunde und Bekannte weitergegeben werden und die andere für alle E-Mail-Angaben im Internet.
- Weitere Informationen zum Thema „So schütze ich meinen Computer“ finden Sie unter www.klicksafe.de (Klicken Sie auf Themen, Technische Schutzmaßnahmen, dann auf Den PC schützen).
- handysektor.de – „12 wichtige Tipps vom handysektor“ (Klicken Sie auf Tipps) www.handysektor.de



► Die Initiative klicksafe ist ein Projekt im Rahmen des Programms „Mehr Sicherheit im Internet“ (Safer Internet Programme) der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Projektkoordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt.

Es wird darauf hingewiesen, dass alle Angaben in diesen Tipps trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der AutorInnen ausgeschlossen ist.



Unveränderte nichtkommerzielle Vervielfältigung und Verbreitung ist ausdrücklich erlaubt unter Angabe der Quelle klicksafe.de und der Webseite www.klicksafe.de.

Siehe: <http://creativecommons.org/licenses/by-nc-nd/3.0/de/>

Coverfoto: © WavebreakMediaMicro - www.fotolia.com

Herausgeber:

klicksafe

c/o Landesanstalt für Medien

Nordrhein-Westfalen (LfM)

Zollhof 2

D-40221 Düsseldorf

T: +49 (0)211-77 00 7- 0

F: +49 (0)211-72 71 70

E: klicksafe@lfm-nrw.de

W: www.klicksafe.de

klicksafe wird gefördert von der Europäischen Union

